MIT Guide to Lock Picking

Ted the Tool

September 1, 1991

Distribution

August 1991 revision.

Contents

Chapter 1

It's Easy

The big secret of lock picking is that it's easy. Anyone can learn how to pick locks.

The theory of lock picking is the theory of exploiting mechanical defects. There are a few basic concepts and definitions but the bulk of the material consists of tricks for opening locks with particular defects or characteristics. The organization of this manual reflects this structure. The first few chapters present the vocabulary and basic information about locks and lock picking. There is no way to learn lock picking without practicing, so one chapter presents a set of carefully chosen exercises that will help you learn the skills of lock picking. The document ends with a catalog of the mechanical traits and defects found in locks and the techniques used to recognize and exploit them. The first appendix describes how to make lock picking tools. The other appendix presents some of the legal issues of lock picking.

The exercises are important. The only way to learn how to recognize and exploit the defects in a lock is to practice. This means practicing many times on the same lock as well as practicing on many different locks. Anyone can learn how to open desk and filing cabinet locks, but the ability to open most locks in under thirty seconds is a skill that requires practice.

Before getting into the details of locks and picking, it is worth pointing out that lock picking is just one way to bypass a lock, though it does cause less damage than brute force techniques. In fact, it may be easier to bypass the bolt mechanism than to bypass the lock. It may also be easier to bypass some other part of the door or even avoid the door entirely. Remember: There is always another way, usually a better one.

Chapter 2

How a Key Opens a Lock

This chapter presents the basic workings of pin tumbler locks, and the vocabulary used in the rest of this booklet. The terms used to describe locks and lock parts vary from manufacture to manufacture and from city to city, so even if you already understand the basic workings of locks, you should look at figure 2.1 for the vocabulary.

Knowing how a lock works when it is opened by a key is only part of what you need to know. You also need to know how a lock responds to picking. Chapters 3 and 5 present models which will help you understand a lock's response to picking.

Figure 2.1 introduces the vocabulary of real locks. The key is inserted into the *keyway* of the *plug*. The protrusions on the side of the keyway are called *wards*. Wards restrict the set of keys that can be inserted into the plug. The plug is a cylinder which can rotate when the proper key is fully inserted. The non-rotating part of the lock is called the *hull*. The first pin touched by the key is called pin one. The remaining pins are numbered increasingly toward the rear of the lock.

The proper key lifts each pin pair until the gap between the *key pin* and the *driver pin* reaches the *sheer line*. When all the pins are in this position, the plug can rotate and the lock can be opened. An incorrect key will leave some of the pins protruding between the hull and the plug, and these pins will prevent the plug from rotating.

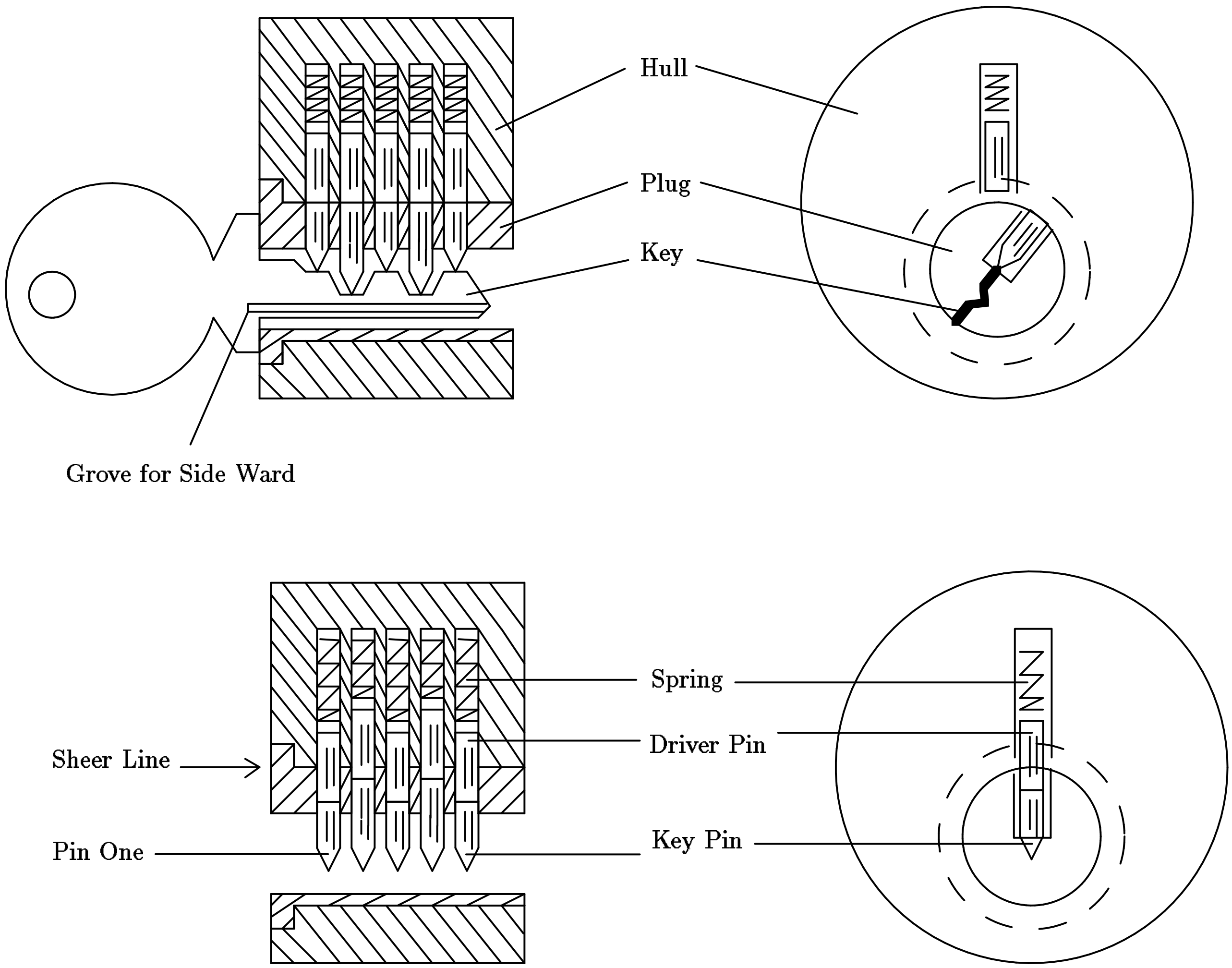


Figure 2.1: Workings of pin tumbler locks

Chapter 3

The Flatland Model

In order to become good at picking locks, you will need a detailed understanding of how locks works and what happens as it is picked. This document uses two models to help you understand the behavior of locks. This chapter presents a model that highlights interactions between pin positions. Chapter 4 uses this model to explain how picking works. Chapter 9 will use this model to explain complicated mechanical defects.

The "flatland" model of a lock is shown in Figure 3.1. This is not a cross section of a real lock. It is a cross section of a very simple kind of lock. The purpose of this lock is to keep two plates of metal from sliding over each other unless the proper key is present. The lock is constructed by placing the two plates over each other and drilling holes which pass through both plates. The figure shows a two hole lock. Two pins are placed in each hole such that the gap between the pins does not line up with the gap between the plates. The bottom pin is called the *key pin* because it touches the key. The top pin is called the *driver pin*. Often the driver and key pins are just called the driver and the pin. A protrusion on the underside of the bottom plate keeps the pins from falling out, and a spring above the top plate pushes down on the driver pin.

If the key is absent, the plates cannot slide over each other because the driver pins pass through both plates. The correct key lifts the pin pairs to align the gap between the pins with the gap between the plates. See Figure 3.3. That is, the key lifts the key pin until its top reaches the lock's sheer line. In this configuration, the plates can slide past each other.

Figure 3.3 also illustrates one of the important features of real locks. There is always a sliding allowance. That is, any parts which slide past each other must be separated by a gap. The gap between the top and bottom plates allows a range of keys to open the lock. Notice that the right key pin in Figure 3.3 is not raised as high as the left pin, yet the lock will still open.

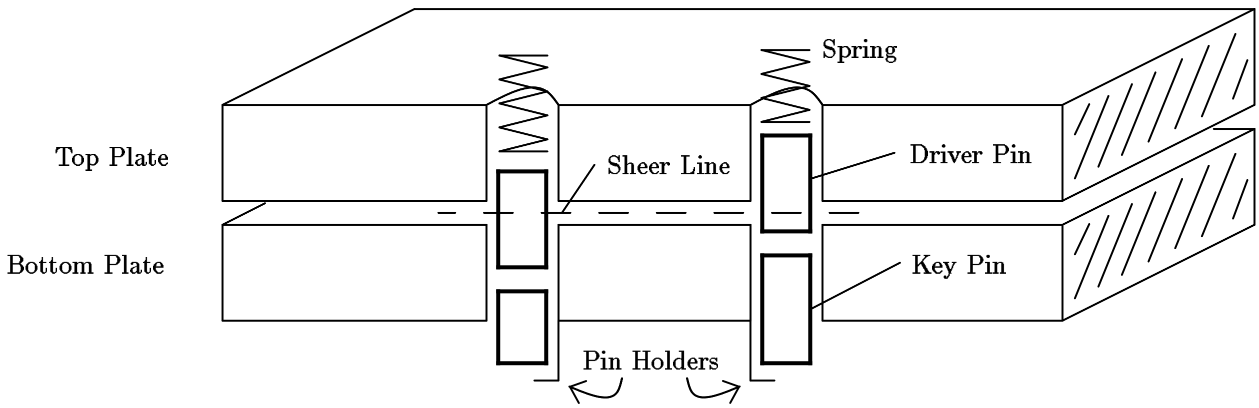


Figure 3.1: Flatland model of a lock

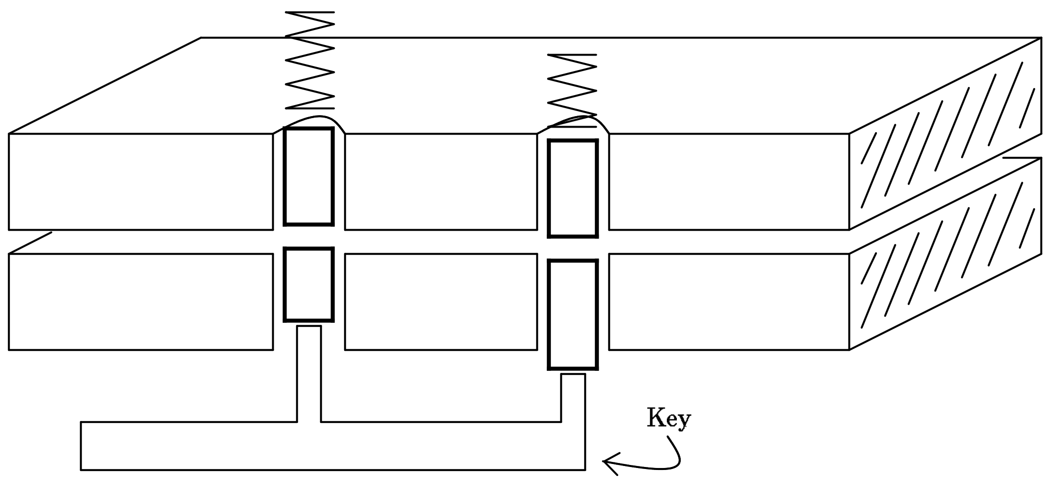


Figure 3.2: (a) Flatland key raises pins

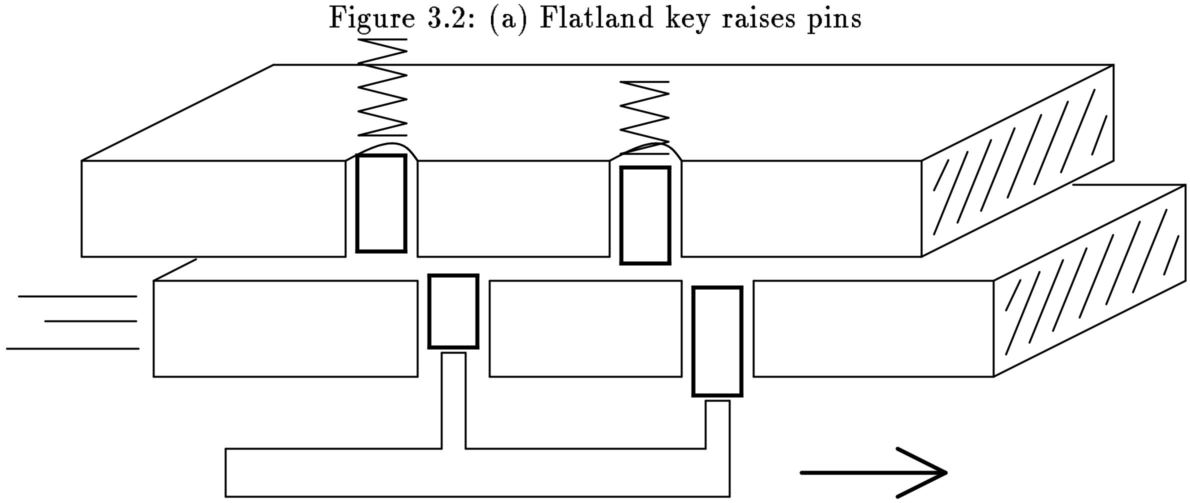


Figure 3.3: (b) Proper key allows plates to slide

Chapter 4

Basic Picking & The Binding Defect

The flatland model highlights the basic defect that enables lock picking to work. This defect makes it possible to open a lock by lifting the pins one at a time, and thus you don't need a key to lift all the pins at the same time. Figure 4.3 shows how the pins of a lock can be set one at a time. The first step of the procedure is to apply a sheer force to the lock by pushing on the bottom plate. This force causes one or more of the pins to be scissored between the top and bottom plate. The most common defect in a lock is that only one pin will bind. Figure 4.3a shows the left pin binding. Even though a pin is binding, it can be pushed up with a picking tool, see Figure 4.3b. When the top of the key pin reaches the sheer line, the bottom plate will slide slightly. If the pick is removed, the driver pin will be held up by the overlapping bottom plate, and the key pin will drop down to its initial position, see Figure 4.3c. The slight movement of the bottom plate causes a new pin to bind. The same procedure can be used to set the new pin.

Thus, the procedure for *one pin at a time picking* a lock is to apply a sheer force, find the pin which is binding the most, and push it up. When the top of the key pin reaches the sheer line, the moving portion of the lock will give slightly, and driver pin will be trapped above the sheer line. This is called *setting* a pin.

Chapter 9 discusses the different defects that cause pins to bind one at a time.

1. Apply a sheer force.
2. Find the pin that is binding the most.
3. Push that pin up until you feel it set at the sheer line.
4. Go to step 2.

Table 4.1: Figure 5: Picking a lock one pin at a time.

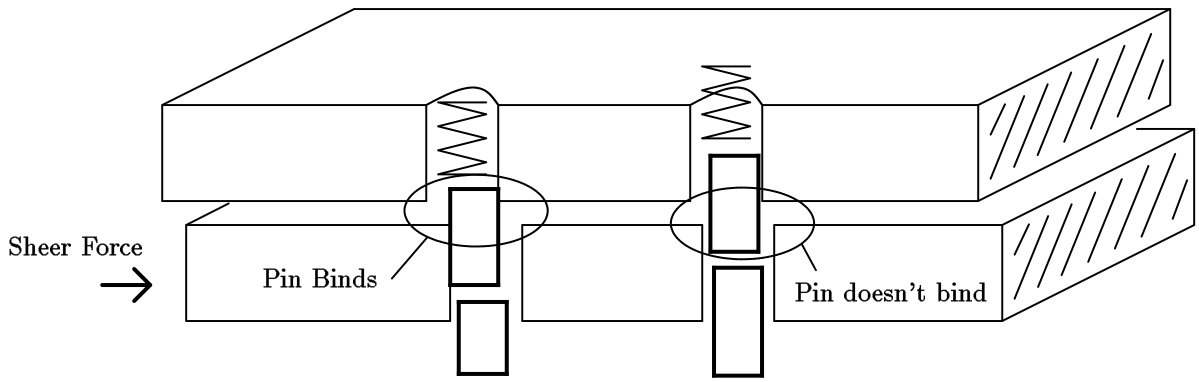


Figure 4.1: (a) Sheer force causes driver to bind

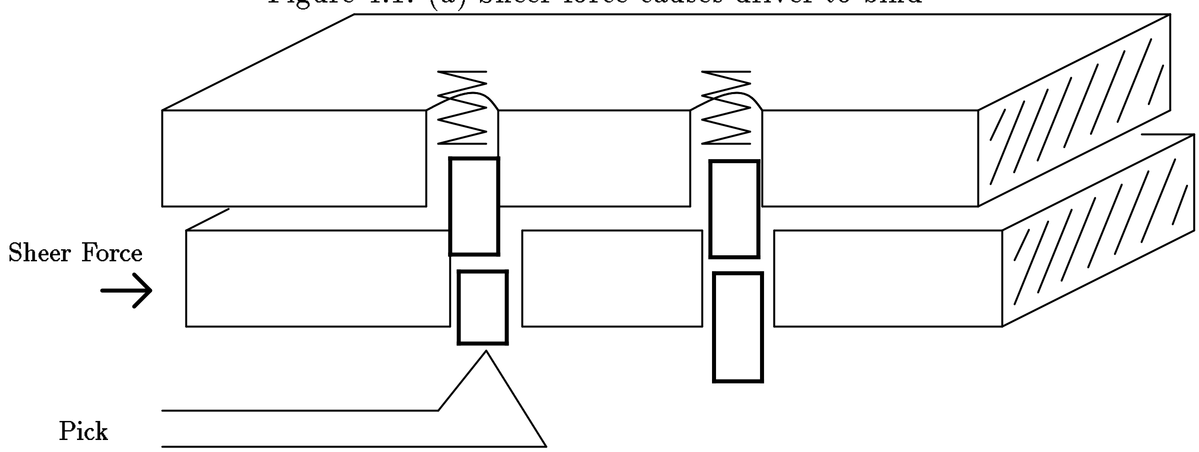


Figure 4.2: (b) Pick lifts the binding pin

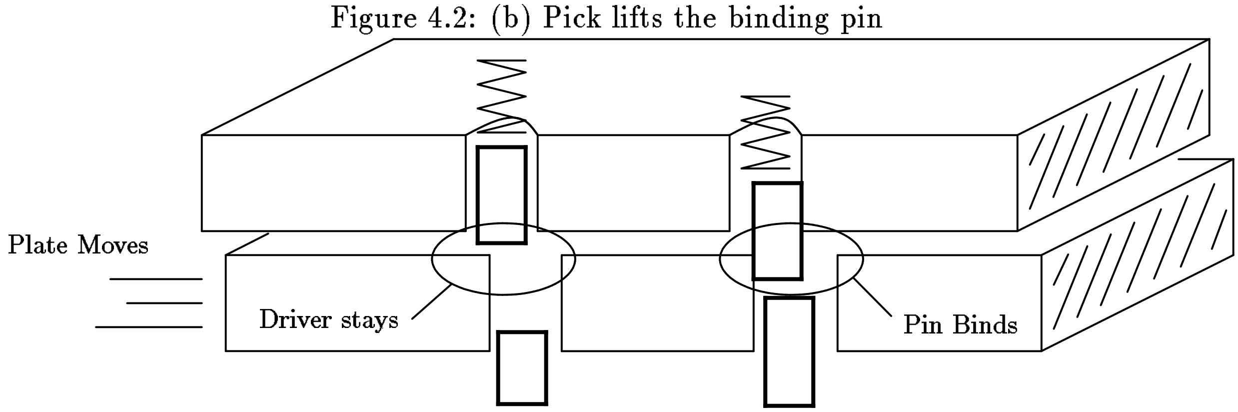


Figure 4.3: (c) Left driver sets and right driver binds

Chapter 5

The Pin Column Model

The flatland model of locks can explain effects that involve more than one pin, but a different model is needed to explain the detailed behavior of a single pin. See Figure 5.1. The pin-column model highlights the relationship between the torque applied and the amount of force needed to lift each pin. It is essential that you understand this relationship.

In order to understand the "feel" of lock picking you need to know how the movement of a pin is effect by the torque applied by your torque wrench (tensioner) and the pressure applied by your pick. A good way to represent this understanding is a graph that shows the minimum pressure needed to move a pin as a function of how far the pin has been displaced from its initial position. The remainder of this chapter will derive that force graph from the pin-column model.

Figure 5.2 shows a single pin position after torque has been applied to the plug. The forces acting of the driver pin are the friction from the sides, the spring contact force from above, and the contact force from the key pin below. The amount of pressure you apply to the pick determines the contact force from below.

The spring force increases as the pins are pushed into the hull, but the increase is slight, so we will assume that the spring force is constant over the range of displacements we are interested in. The pins will not move unless you apply enough pressure to overcome the spring force. The binding friction is proportional to how hard the driver pin is being scissored between the plug and the hull, which in this case is proportional to the torque. The more torque you apply to the plug, the harder it will be to move the pins. To make a pin move, you need to apply a pressure that is greater than the sum of the spring and friction forces.

When the bottom of the driver pin reaches the sheer line, the situation suddenly changes. See Figure 5.3. The friction binding force drops to zero and the plug rotates slightly (until some other pin binds). Now the only resistance to motion is the spring force. After the top of the key pin crosses the gap between the plug and the hull, a new contact force arises from the key pin striking the hull. This force can be quite large, and it causes a peak in the amount of pressure needed to move a pin.

If the pins are pushed further into the hull, the key pin acquires a binding fiction like the driver pin had in the initial situation. See Figure 5.4. Thus, the amount of pressure needed

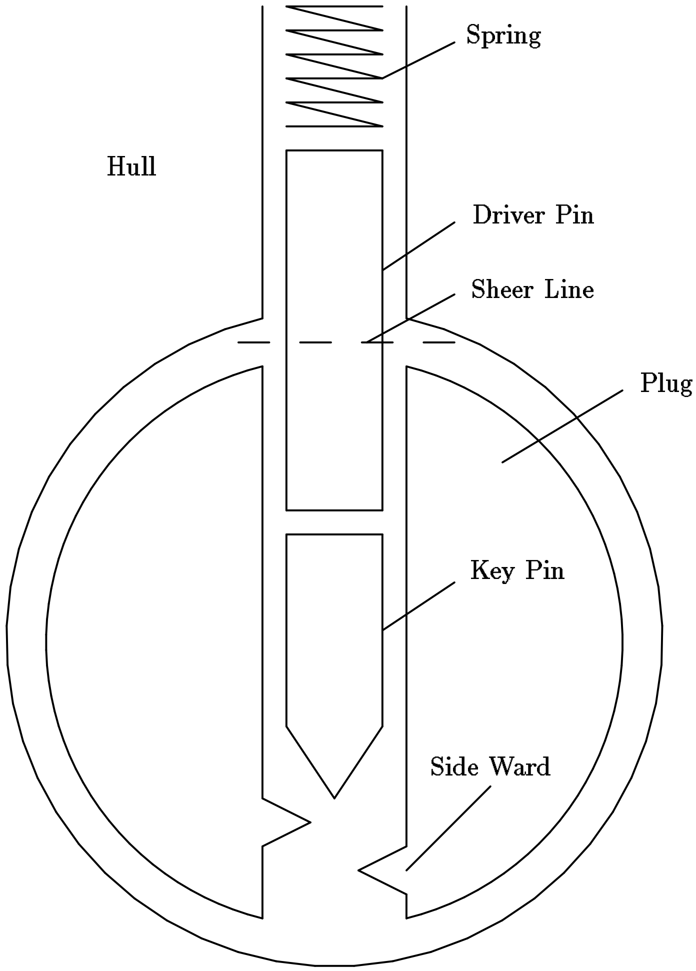


Figure 5.1: The pin-column model

to move the pins before and after the sheer line is about the same. Increasing the torque increases the required pressure. At the sheer line, the pressure increases dramatically due to the key pin hitting the hull. This analysis is summarized graphically in figure 5.5.

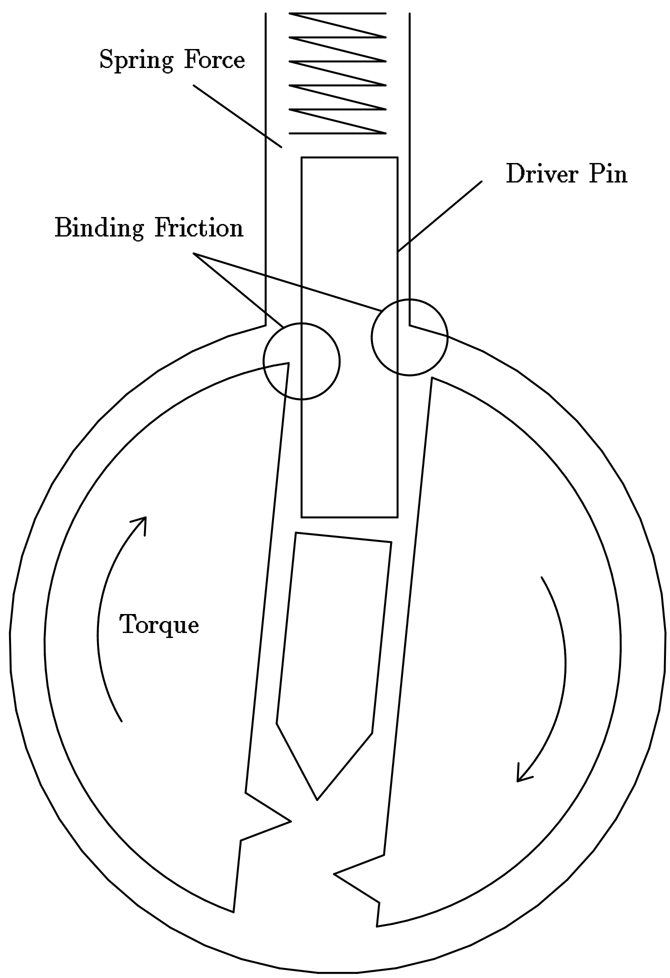


Figure 5.2: Binding in the pin-column model

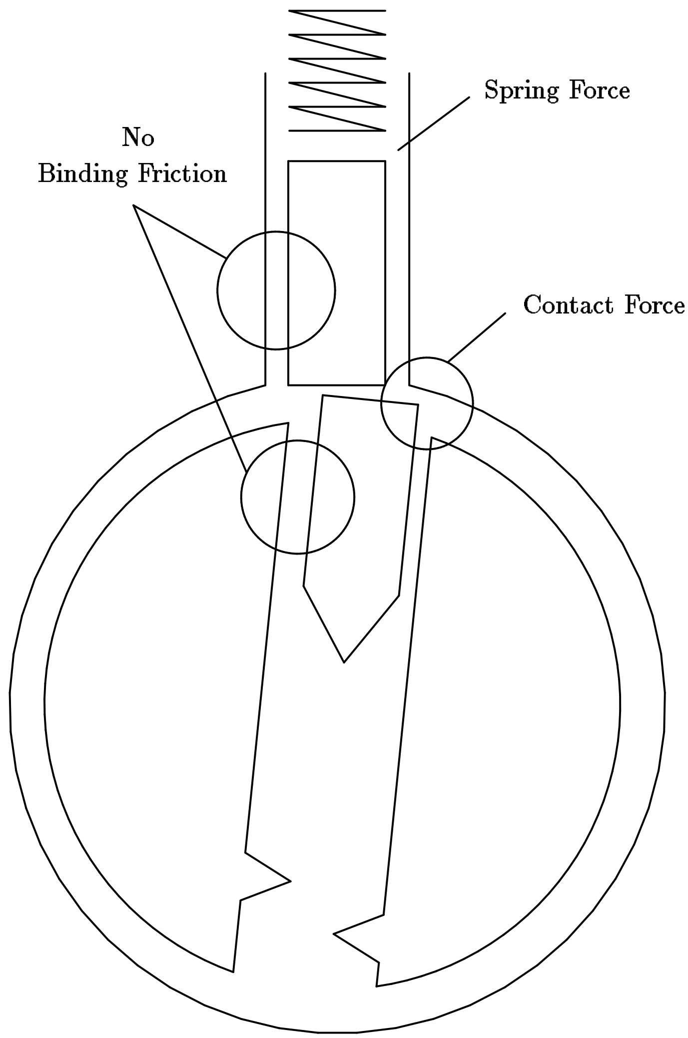


Figure 5.3: Pins at the sheer line

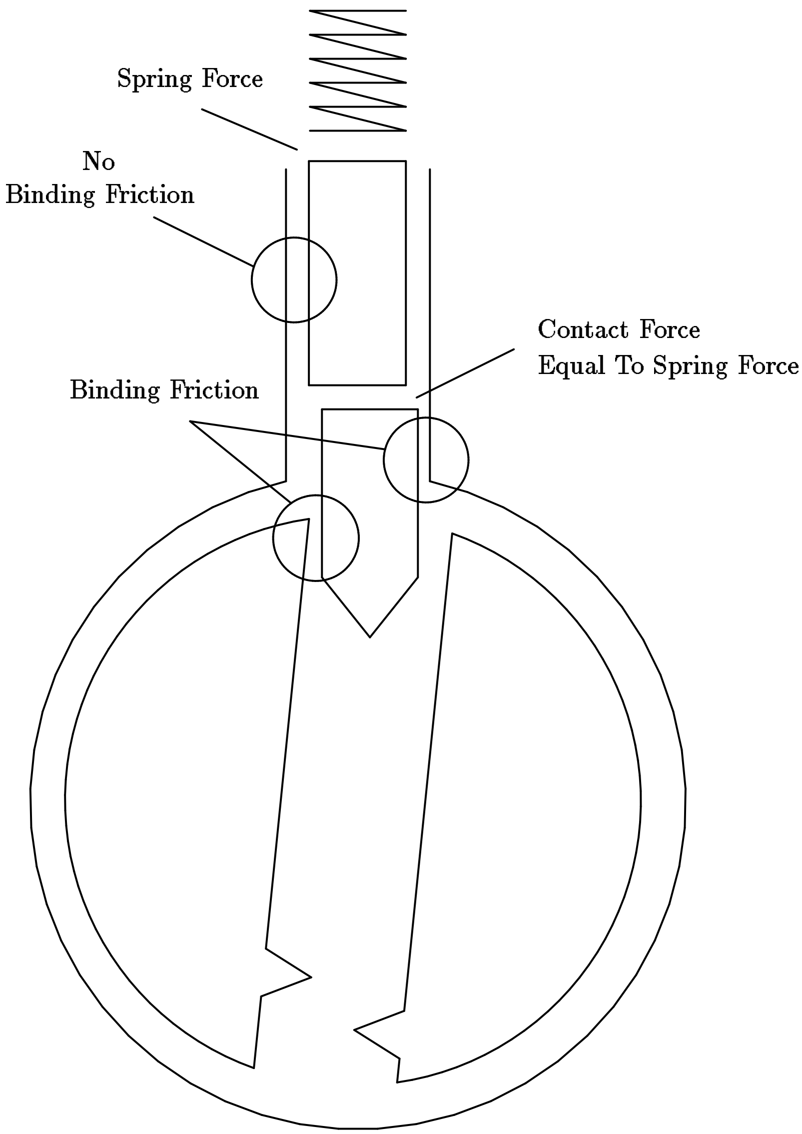


Figure 5.4: Key pin enters hull

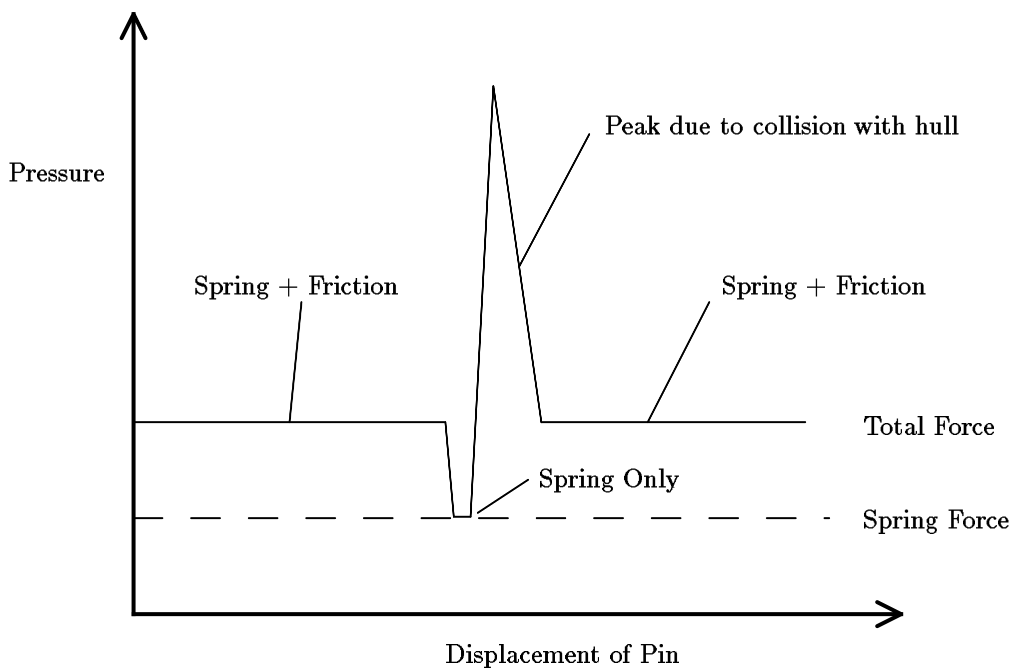


Figure 5.5: Pressure required to move pins

Chapter 6

Basic Scrubbing

At home you can take your time picking a lock, but in the field, speed is always essential. This chapter presents a lock picking technique called *scrubbing* that can quickly open most locks.

The slow step in basic picking (chapter 4) is locating the pin which is binding the most. The force diagram (Figure 5.5) developed in chapter 5 suggests a fast way to select the correct pin to lift. Assume that all the pins could be characterized by the same force diagram. That is, assume that they all bind at once and that they all encounter the same friction. Now consider the effect of running the pick over all the pins with a pressure that is great enough to overcome the spring and friction forces but not great enough to overcome the collision force of the key pin hitting the hull. Any pressure that is above the flat portion of the force graph and below the top of the peak will work. As the pick passes over a pin, the pin will rise until it hits the hull, but it will not enter the hull. See Figure 5.3. The collision force at the sheer line resists the pressure of the pick, so the pick rides over the pin without pressing it into the hull. If the proper torque is being applied, the plug will rotate slightly. As the pick leaves the pin, the key pin will fall back to its initial position, but the driver pin will catch on the edge of the plug and stay above the sheer line. See figure 6.1. In theory one stroke of the pick over the pins will cause the lock to open.

In practice, at most one or two pins will set during a single stroke of the pick, so several strokes are necessary. Basically, you use the pick to scrub back and forth over the pins while you adjust the amount of torque on the plug. The exercises in chapter 8 will teach you how to choose the correct torque and pressure.

You will find that the pins of a lock tend to set in a particular order. Many factors effect this order (see chapter 9), but the primary cause is a misalignment between the center axis of the plug and the axis on which the holes were drilled. See figure 6.2. If the axis of the pin holes is skewed from the center line of the plug, then the pins will set from back to front if the plug is turned one way, and from front to back if the plug is turned the other way. Many locks have this defect.

Scrubbing is fast because you don't need to pay attention to individual pins. You only need to find the correct torque and pressure. Figure 6.1 summarizes the steps of picking a lock by scrubbing. The exercises will teach you how to recognize when a pin is set and how

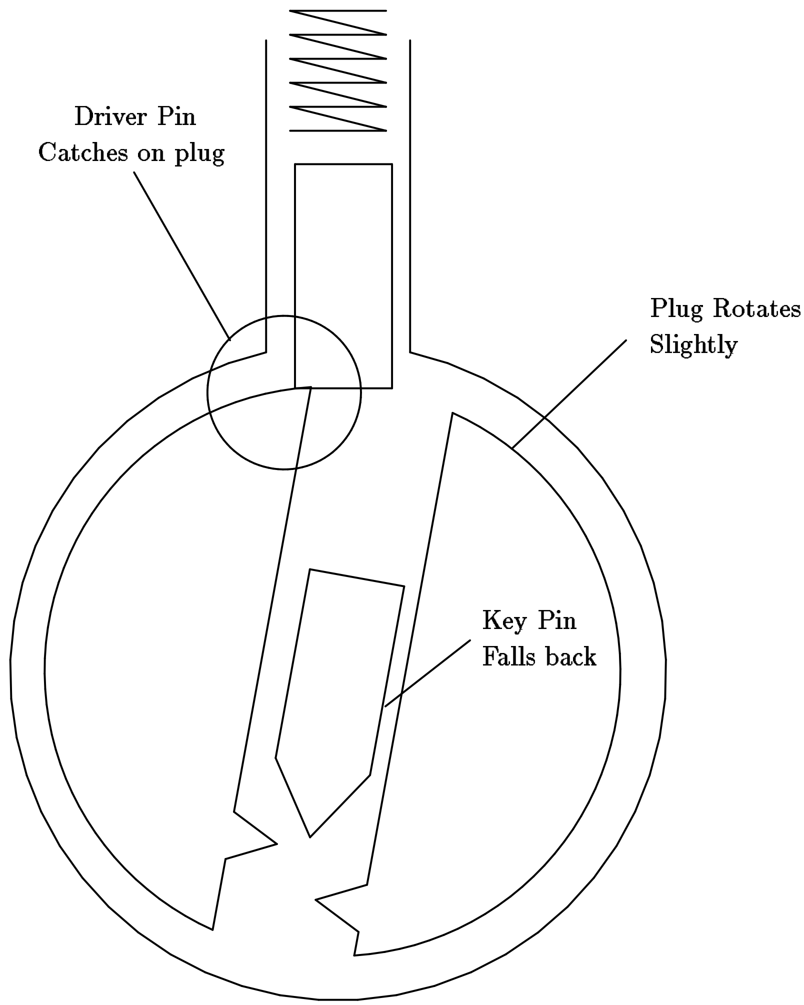


Figure 6.1: Driver pin catches on plug

to apply the correct forces. If a lock doesn't open quickly, then it probably has one of the characteristics described in chapter 9 and you will have to concentrate on individual pins.

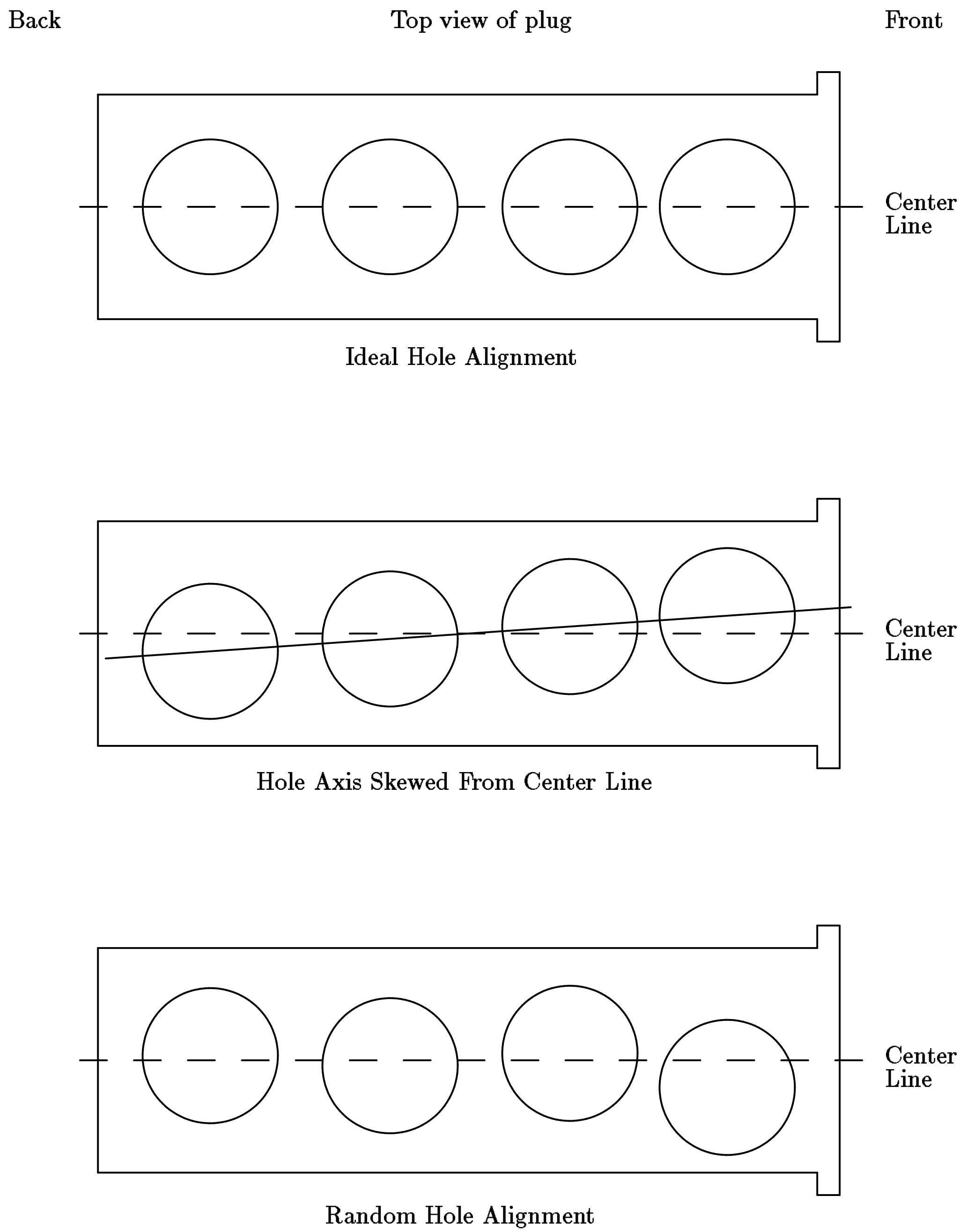


Figure 6.2: Alignment of plug holes

1. Insert the pick and torque wrench. Without applying any torque pull the pick out to get a feel for the stiffness of the lock's springs.

2. Apply a light torque. Insert the pick without touching the pins. As you pull the pick out, apply pressure to the pins. The pressure should be slightly larger than the minimum necessary to overcome the spring force.

3. Gradually increase the torque with each stroke of the pick until pins begin to set.

4. Keeping the torque fixed, scrub back and forth over the pins that have not set. If additional pins do not set, release the torque and start over with the torque found in the last step.

5. Once the majority of the pins have been set, increase the torque and scrub the pins with a slightly larger pressure. This will set any pins which have set low due to beveled edges, etc.

Table 6.1: Figure 13: Basic scrubbing.

Chapter 7

Advanced Lock Picking

Simple lock picking is a trade that anyone can learn. However, advanced lock picking is a craft that requires mechanical sensitivity, physical dexterity, visual concentration and analytic thinking. If you strive to excel at lock picking, you will grow in many ways.

7.1 Mechanical Skills

Learning how to pull the pick over the pins is surprisingly difficult. The problem is that the mechanical skills you learned early in life involved maintaining a fixed position or fixed path for your hands independent of the amount of force required. In lock picking, you must learn how to apply a fixed force independent of the position of your hand. As you pull the pick out of the lock you want to apply a fixed pressure on the pins. The pick should bounce up and down in the keyway according to the resistance offered by each pin.

To pick a lock you need feedback about the effects of your manipulations. To get the feedback, you must train yourself to be sensitive to the sound and feel of the pick passing over the pins. This is a mechanical skill that can only be learned with practice. The exercises will help you recognize the important information coming from your fingers.

7.2 Zen and the Art of Lock Picking

In order to excel at lock picking, you must train yourself to have a visually reconstructive imagination. The idea is to use information from all your senses to build a picture of what is happening inside the lock as you pick it. Basically, you want to project your senses into the lock to receive a full picture of how it is responding to your manipulations. Once you have learned how to build this picture, it is easy to choose manipulations that will open the lock.

All your senses provide information about the lock. Touch and sound provide the most information, but the other senses can reveal critical information. For example, your nose can tell you whether a lock has been lubricated recently. As a beginner, you will need to use

your eyes for hand-eye coordination, but as you improve you will find it unnecessary to look at the lock. In fact, it is better to ignore your eyes and use your sight to build an image of the lock based on the information you receive from your fingers and ears.

The goal of this mental skill is to acquire a relaxed concentration on the lock. Don't force the concentration. Try to ignore the sensations and thoughts that are not related to the lock. Don't try to focus on the lock.

7.3 Analytic Thinking

Each lock has its own special characteristics which make picking harder or easier. If you learn to recognize and exploit the "personality traits" of locks, picking will go much faster. Basically, you want to analyze the feedback you get from a lock to diagnose its personality traits and then use your experience to decide on an approach to open the lock. Chapter 9 discusses a large number of common traits and ways to exploit or overcome them.

People underestimate the analytic skills involved in lock picking. They think that the picking tool opens the lock. To them the torque wrench is a passive tool that just puts the lock under the desired stress. Let me propose another way to view the situation. The pick is just running over the pins to get information about the lock. Based on an analysis that information the torque is adjusted to make the pins set at the sheer line. It's the torque wrench that opens the lock.

Varying the torque as the pick moves in and out of the keyway is a general trick that can be used to get around several picking problems. For example, if the middle pins are set, but the end pins are not, you can increase the torque as the pick moves over the middle pins. This will reduce the chances of disturbing the correctly set pins. If some pin doesn't seem to lift up far enough as the pick passes over it, then try reducing the torque on the next pass.

The skill of adjusting the torque while the pick is moving requires careful coordination between your hands, but as you become better at visualizing the process of picking a lock, you will become better at this important skill.

Chapter 8

Exercises

This chapter presents a series of exercises that will help you learn the basic skill of lock picking. Some exercises teach a single skill, while others stress the coordination of skills.

When you do these exercises, focus on the skills, not on opening the lock. If you focus on opening the lock, you will get frustrated and your mind will stop learning. The goal of each exercise is to learn something about the particular lock you are holding and something about yourself. If a lock happens to open, focus on the memory of what you were doing and what you felt just before it opened.

These exercises should be practiced in short sessions. After about thirty minutes you will find that your fingers become sore and your mind looses its ability to achieve relaxed concentration.

8.1 Exercise 1: Bouncing the pick

This exercise helps you learn the skill of applying a fixed pressure with the pick independent of how the pick moves up and down in the lock. Basically you want to learn how to let the pick bounce up and down according to the resistance offered by each pin.

How you hold the pick makes a difference on how easy it is to apply a fixed pressure. You want to hold it in such a way that the pressure comes from your fingers or your wrist. Your elbow and shoulder do not have the dexterity required to pick locks. While you are scrubbing a lock notice which of your joints are fixed, and which are allowed to move. The moving joints are providing the pressure.

One way to hold a pick is to use two fingers to provide a pivot point while another finger levers the pick to provide the pressure. Which fingers you use is a matter of personal choice. Another way to hold the pick is like holding a pencil. With this method, your wrist provides the pressure. If your wrist is providing the pressure, your shoulder and elbow should provide the force to move the pick in and out of the lock. Do not use your wrist to both move the pick and apply pressure.

A good way to get used to the feel of the pick bouncing up and down in the keyway is to try scrubbing over the pins of an open lock. The pins cannot be pushed down, so the pick

must adjust to the heights of the pins. Try to feel the pins rattle as the pick moves over them. If you move the pick quickly, you can hear the rattle. This same rattling feel will help you recognize when a pin is set correctly. If a pin appears to be set but it doesn't rattle, then it is false set. False set pins can be fixed by pushing them down farther, or by releasing torque and letting them pop back to their initial position.

One last word of advice. Focus on the tip of the pick. Don't think about how you are moving the handle; think about how you are moving the tip of the pick.

8.2 Exercise 2: Picking pressure

This exercise will teach you the range of pressures you will need to apply with a pick. When you are starting, just apply pressure when you are drawing the pick out of the lock. Once you have mastered that, try applying pressure when the pick is moving inward.

With the flat side of your pick, push down on the first pin of a lock. Don't apply any torque to the lock. The amount of pressure you are applying should be just enough to overcome the spring force. This force gives you an idea of minimum pressure you will apply with a pick.

The spring force increases as you push the pin down. See if you can feel this increase.

Now see how it feels to push down the other pins as you pull the pick out of the lock. Start out with both the pick and torque wrench in the lock, but don't apply any torque. As you draw the pick out of the lock, apply enough pressure to push each pin all the way down.

The pins should spring back as the pick goes past them. Notice the sound that the pins make as they spring back. Notice the popping feel as a pick goes past each pin. Notice the springy feel as the pick pushes down on each new pin.

To help you focus on these sensations, try counting the number of pins in the lock. Door locks at MIT have seven pins, padlocks usually have four.

To get an idea of the maximum pressure, use the flat side of your pick to push down all the pins in the lock. Sometimes you will need to apply this much pressure to a single pin. If you encounter a new kind of lock, perform this exercise to determine the stiffness of its springs.

8.3 Exercise 3: Picking Torque

This exercise will teach you the range of torque you will need to apply to a lock. It demonstrates the interaction between torque and pressure which was describe in chapter 5.

The minimum torque you will use is just enough to overcome the fiction of rotating the plug in the hull. Use your torque wrench to rotate the plug until it stops. Notice how much torque is needed to move the plug before the pins bind. This force can be quite high for locks that have been left out in the rain. The minimum torque for padlocks includes the force of a spring that is attached between the plug and the shackle bolt.

To get a feel for the maximum value of torque, use the flat side of the pick to push all the pins down, and try applying enough torque to make the pins stay down after the pick is removed. If your torque wrench has a twist in it, you may not be able to hold down more than a few pins.

If you use too much torque and too much pressure you can get into a situation like the one you just created. The key pins are pushed too far into the hull and the torque is sufficient to hold them there.

The range of picking torque can be found by gradually increasing the torque while scrubbing the pins with the pick. Some of the pins will become harder to push down. Gradually increase the torque until some of the pins set. These pins will loose their springiness. Keeping the torque fixed, use the pick to scrub the pins a few times to see if other pins will set.

The most common mistake of beginners is to use too much torque. Use this exercise to find the minimum torque required to pick the lock.

8.4 Exercise 4: Identifying Set Pins

While you are picking a lock, try to identify which pins are set. You can tell a pin is set because it will have a slight give. That is, the pin can be pushed down a short distance with a light pressure, but it becomes hard to move after that distance (see chapter 6 for an explanation). When you remove the light pressure, the pin springs back up slightly. Set pins also rattle if you flick them with the pick. Try listening for that sound.

Run the pick over the pins and try to decide whether the set pins are in the front or back of the lock (or both). Try identifying exactly which pins are set. Remember that pin one is the frontmost pin (i.e., the pin that a key touches first). The most important skill of lock picking is the ability to recognize correctly set pins. This exercise will teach you that skill.

Try repeating this exercise with the plug turning in the other direction. If the front pins set when the plug is turned one way, the back pins will set when the plug is turned the other way. See Figure 6.2 for an explanation.

One way to verify how many pins are set is to release the torque, and count the clicks as the pins snap back to their initial position. Try this. Try to notice the difference in sound between the snap of a single pin and the snap of two pins at once. A pin that has been false set will also make a snapping sound.

Try this exercise with different amounts of torque and pressure. You should notice that a larger torque requires a larger pressure to make pins set correctly. If the pressure is too high, the pins will be jammed into the hull and stay there.

8.5 Exercise 5: Projection

As you are doing the exercises try building a picture in your mind of what is going on. The picture does not have to be visual, it could be a rough understanding of which pins are set

and how much resistance you are encountering from each pin. One way to foster this picture building is to try to remember your sensations and beliefs about a lock just before it opened. When a lock opens, don't think "that's over", think "what happened".

This exercise requires a lock that you find easy to pick. It will help you refine the visual skills you need to master lock picking. Pick the lock, and try to remember how the process felt. Rehearse in your mind how everything feels when the lock is picked properly. Basically, you want to create a movie that records the process of picking the lock. Visualize the motion of your muscles as they apply the correct pressure and torque, and feel the resistance encountered by the pick. Now pick the lock again trying to match your actions to the movie.

By repeating this exercise, you are learning how to formulate detailed commands for your muscles and how to interpret feedback from your senses. The mental rehearsal teaches you how to build a visual understanding of the lock and how to recognize the major steps of picking it.

Chapter 9

Recognizing and Exploiting Personality Traits

Real locks have a wide range of mechanical features and defects that help and hinder lock picking. If a lock doesn't respond to scrubbing, then it probably has one of the traits discussed in this chapter. To open the lock, you must diagnose the trait and apply the recommended technique. The exercises will help you develop the mechanical sensitivity and dexterity necessary to recognize and exploit the different traits.

9.1 Which Way To Turn

It can be very frustrating to spend a long time picking a lock and then discover that you turned the plug the wrong way. If you turn a plug the wrong way it will rotate freely until it hits a stop, or until it rotates 180 degrees and the drivers enter the keyway (see section 9.11). Section 9.11 also explains how to turn the plug more than 180 degrees if that is necessary to fully retract the bolt. When the plug is turned in the correct direction, you should feel an extra resistance when the plug cam engages the bolt spring.

The direction to turn the plug depends on the bolt mechanism, not on the lock, but here are some general rules. Cheap padlocks will open if the plug is turned in either direction, so you can chose the direction which is best for the torque wrench. All padlocks made by the Master company can be opened in either direction. Padlocks made by Yale will only open if the plug is turned clockwise. The double plug Yale cylinder locks generally open by turning the bottom of the keyway (i.e., the flat edge of the key) away from the nearest doorframe. Single plug cylinder locks also follow this rule. See Figure 9.1. Locks built into the doorknob usually open clockwise. Desk and filing cabinet locks also tend to open clockwise.

When you encounter a new kind of lock mechanism, try turning the plug in both directions. In the correct direction, the plug will be stopped by the pins, so the stop will feel mushy when you use heavy torque. In the wrong direction the plug will be stopped by a metal tab, so the stop will feel solid.

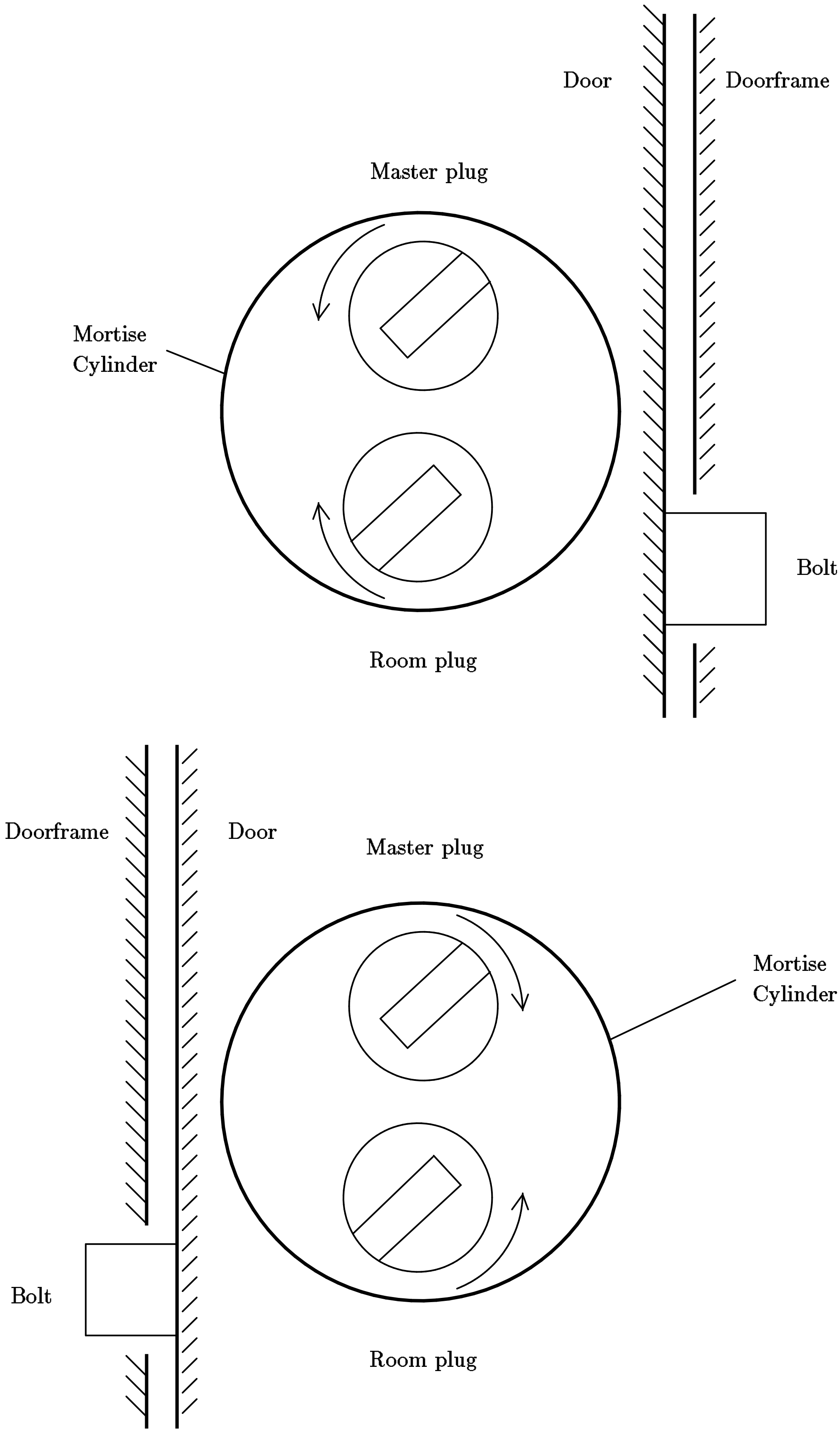


Figure 9.1: Direction to turn plug

9.2 How Far to Turn

The companion question to which way to turn a lock is how far to turn it. Desk and filing cabinet locks generally open with less than a quarter turn (90 degrees) of the plug. When opening a desk lock try to avoid having the plug lock in the open position. Locks built into doorknobs also tend to open with less than a quarter turn. Locks which are separate from the doorknob tend to require a half turn to open. Deadbolt lock mechanisms can require almost a full turn to open.

Turning a lock more than 180 degrees is a difficult because the drivers enter the bottom of the keyway. See section 9.11.

9.3 Gravity

Picking a lock that has the springs at the top is different than picking one with the springs at the bottom. It should be obvious how to tell the two apart. The nice feature of a lock with the springs at the bottom is that gravity holds the key pins down once they set. With the set pins out of the way, it is easy to find and manipulate the remaining unset pins. It is also straight forward to test for the slight give of a correctly set pin. When the springs are on top, gravity will pull the key pins down after the driver pin catches at the sheer line. In this case, you can identify the set pins by noticing that the key pin is easy to lift and that it does not feel springy. Set pins also rattle as you draw the pick over them because they are not being pushed down by the driver pin.

9.4 Pins Not Setting

If you scrub a lock and pins are not setting even when you vary the torque, then some pin has false set and it is keeping the rest of the pins from setting. Consider a lock whose pins prefer to set from back to front. If the backmost pin false sets high or low (see Figure 9.2), then the plug cannot rotate enough to allow the other pins to bind. It is hard to recognize that a back pin has false set because the springiness of the front pins makes it hard to sense the small give of a correctly set back pin. The main symptom of this situation is that the other pins will not set unless a very large torque is applied.

When you encounter this situation, release the torque and start over by concentrating on the back pins. Try a light torque and moderate pressure, or heavy torque and heavy pressure. Try to feel for the click that happens when a pin reaches the sheer line and the plug rotates slightly. The click will be easier to feel if you use a stiff torque wrench.

9.5 Elastic Deformation

The interesting events of lock picking happen over distances measured in thousandths of an inch. Over such short distances, metals behave like springs. Very little force is necessary

to deflect a piece metal over those distances, and when the force is removed, the metal will spring back to its original position.

Deformation can be used to your advantage if you want to force several pins to bind at once. For example, picking a lock with pins that prefer to set from front to back is slow because the pins set one at a time. This is particularly true if you only apply pressure as the pick is drawn out of the lock. Each pass of the pick will only set the frontmost pin that is binding. Numerous passes are required to set all the pins. If the preference for setting is not very strong (i.e., the axis of the plug holes is only slightly skewed from the plug's center line), then you can cause additional pins to bind by applying extra torque. Basically, the torque puts a twist in the plug that causes the front of the plug to be deflected further than the back of the plug. With light torque, the back of the plug stays in its initial position, but with medium to heavy torque, the front pin columns bend enough to allow the back of the plug to rotate and thus cause the back pins to bind. With the extra torque, a single stroke of the pick can set several pins, and the lock can be opened quickly. Too much torque causes its own problems.

When the torque is large, the front pins and plug holes can be deformed enough to prevent the pins from setting correctly. In particular, the first pin tends to false set low. Figure 9.2 shows how excess torque can deform the bottom of the driver pin and prevent the key pin from reaching the sheer line. This situation can be recognized by the lack of give in the first pin. Correctly set pins feel springy if they are pressed down slightly. A falsely set pin lacks this springiness. The solution is to press down hard on the first pin. You may want to reduce the torque slightly, but if you reduce torque too much then other pins will unset as the first pin is being depressed.

It is also possible to deform the top of the key pin. The key pin is scissored between the plug and the hull and stays fixed. When this happens, the pin is said to be false set high.

9.6 Loose Plug

The plug is held into the hull by being wider at the front and by having a cam on the back that is bigger than the hole drilled into the hull. If the cam is not properly installed, the plug can move in and out of the lock slightly. On the outward stroke of the pick, the plug will move forward, and if you apply pressure on the inward stroke, the plug will be pushed back.

The problem with a loose plug is that the driver pins tend to set on the back of the plug holes rather than on the sides of the holes. When you push the plug in, the drivers will unset. You can use this defect to your advantage by only applying pressure on the outward or inward stroke of the pick. Alternatively, you can use your finger or torque wrench to prevent the plug from moving forward.

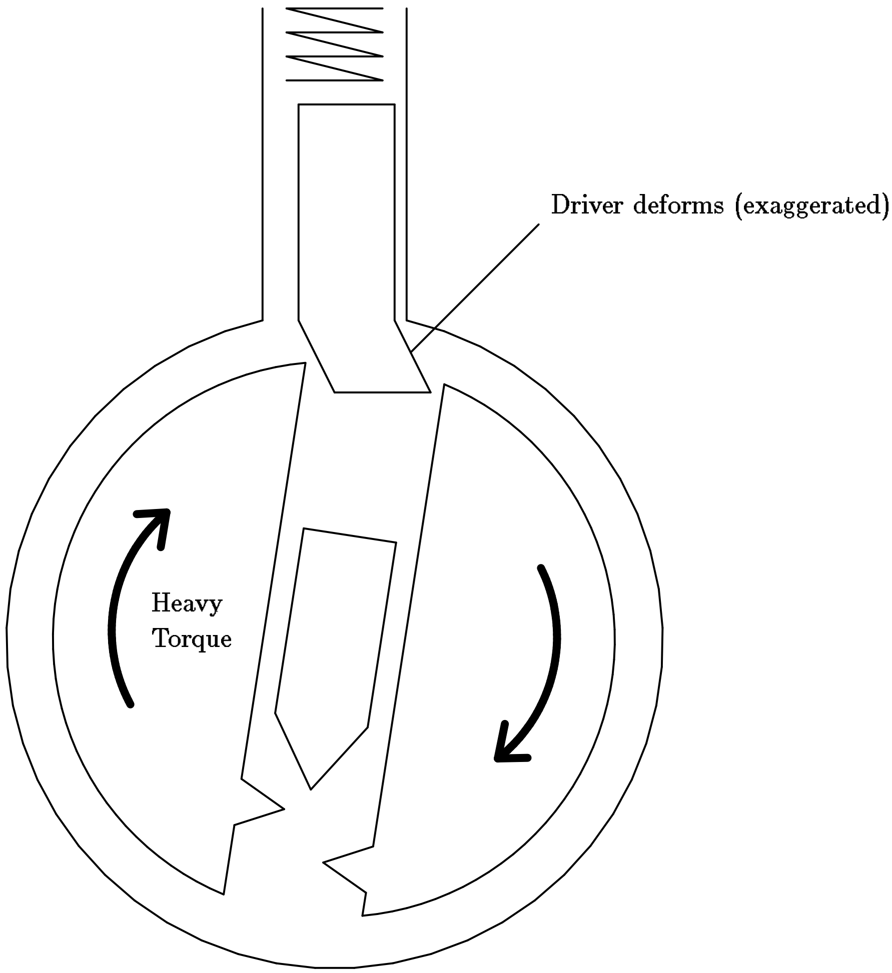


Figure 9.2: Driver pin false set by elastic deformation

9.7 Pin Diameter

When the pair of pins in a particular column have different diameters, that column will react strangely to the pressure of the pick.

The top half of Figure 9.3 shows a pin column with a driver pin that has a larger diameter than the key pin. As the pins are lifted, the picking pressure is resisted by the binding friction and the spring force. Once the driver clears the sheer line, the plug rotates (until some other pin binds) and the only resistance to motion is the spring force. If the key pin is small enough and the plug did not rotate very far, the key pin can enter the hull without colliding with the edge of the hull. Some other pin is binding, so again the only resistance to motion is the spring force. This relationship is graphed in the bottom half of the Figure. Basically, the pins feel normal at first, but then the lock clicks and the pin becomes springy. The narrow key pin can be pushed all the way into the hull without loosing its springiness, but when the picking pressure is released, the key pin will fall back to its initial position while the large driver catches on the edge of the plug hole.

The problem with a large driver pin is that the key pin tends to get stuck in the hull when some other pin sets. Imagine that a neighboring pin sets and the plug rotates enough to bind the narrow key pin. If the pick was pressing down on the narrow key pin at the same time as it was pressing down on the pin that set, then the narrow key pin will be in the hull and it will get stuck there when the plug rotates.

The behavior of a large key pin is left as an exercise for the reader.

9.8 Beveled Holes and Rounded pins

Some lock manufacturers (e.g., Yale) bevel the edges of the plug holes and/or round off the ends of the key pins. This tends to reduce the wear on the lock and it can both help and hinder lock picking. You can recognize a lock with these features by the large give in set pins. See Figure 9.4. That is, the distance between the height at which the driver pin catches on the edge of the plug hole and the height at which the key pin hits the hull is larger (sometimes as large as a sixteenth of an inch) when the plug holes are beveled or the pins are rounded. While the key pin is moving between those two heights, the only resistance to motion will be the force of the spring. There won't be any binding friction. This corresponds to the dip in the force graph shown in Figure 5.5.

A lock with beveled plug holes requires more scrubbing to open than a lock without beveled holes because the driver pins set on the bevel instead of setting on the top of the plug. The plug will not turn if one of the drivers is caught on a bevel. The key pin must be scrubbed again to push the driver pin up and off the bevel. The left driver pin in Figure 9.6a is set. The driver is resting on the bevel, and the bottom plate has moved enough to allow the right driver to bind. Figure 9.6b shows what happens after the right driver pin sets. The bottom plate slides further to the right and now the left driver pin is scissored between the bevel and the top plate. It is caught on the bevel. To open the lock, the left driver pin must be pushed up above the bevel. Once that driver is free, the bottom plate

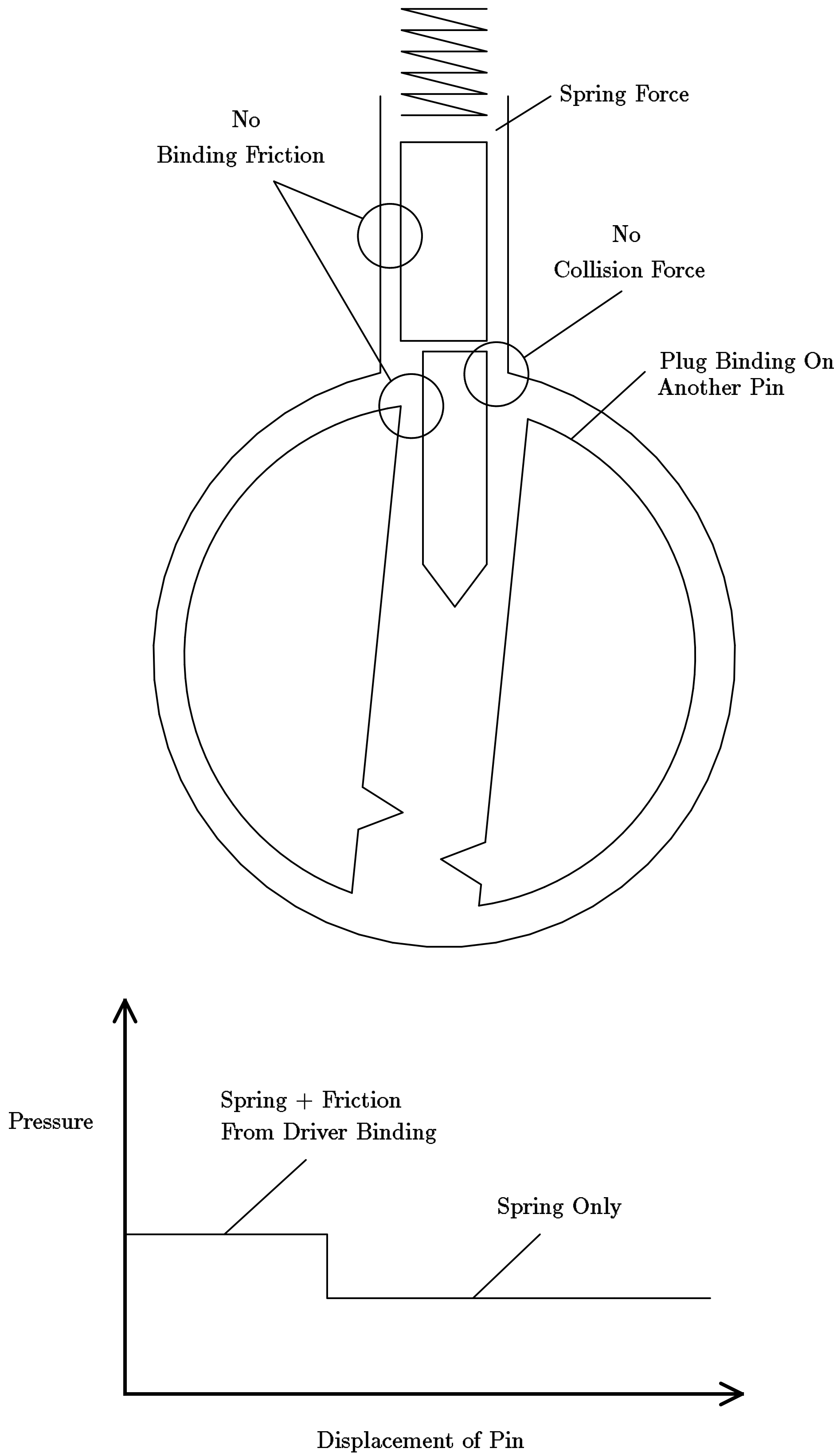


Figure 9.3: Driver pin wider than key pin

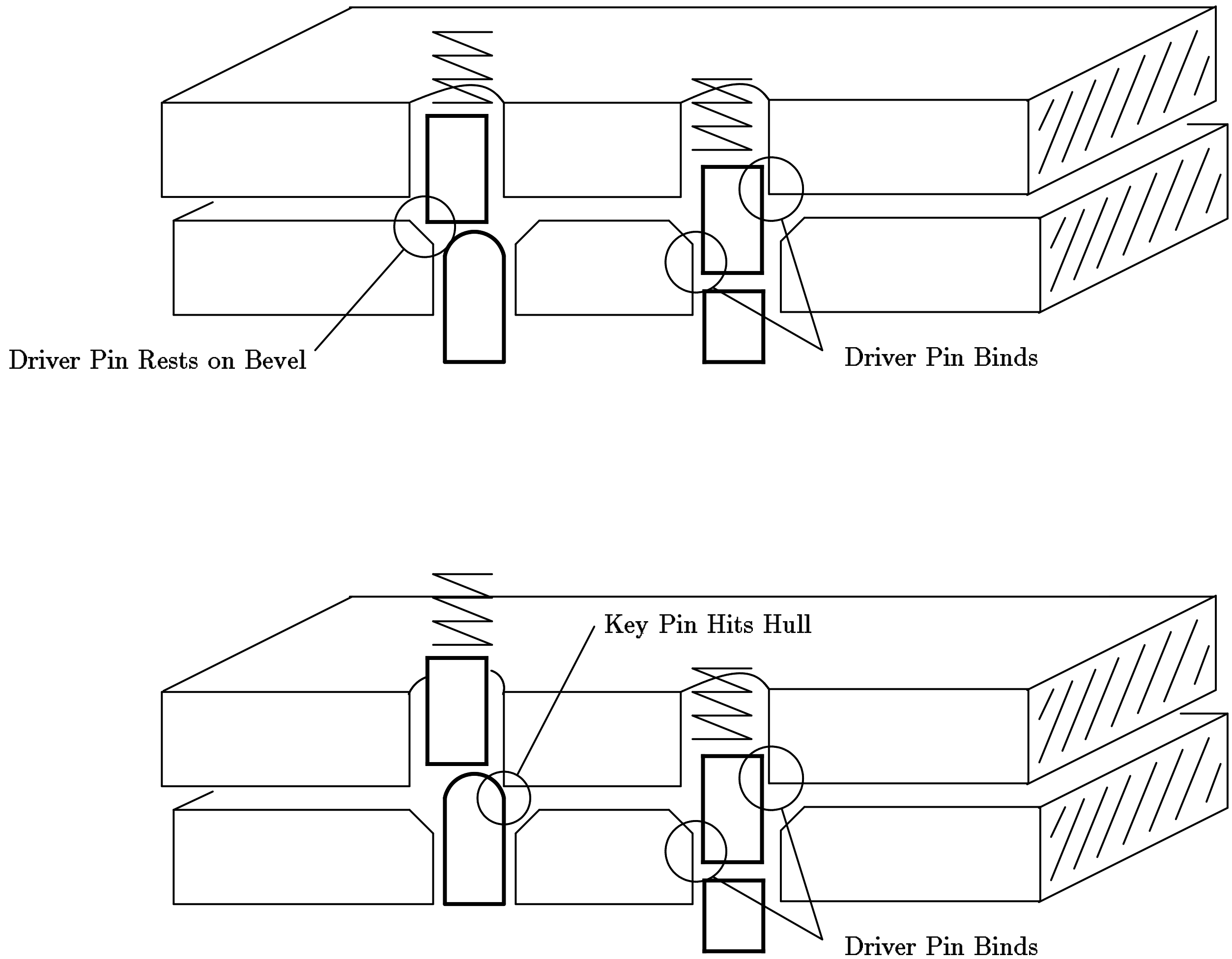


Figure 9.4: Beveled plug holes and rounded key pins

can slide and the right driver may bind on its bevel.

If you encounter a lock with beveled plug holes, and all the pins appear to be set but the lock is not opening, you should reduce torque and continue scrubbing over the pins. The reduced torque will make it easier to push the drivers off the bevels. If pins unset when you reduce the torque, try increasing the torque and the picking pressure. The problem with increasing the force is that you may jam some key pins into the hull.

9.9 Mushroom Driver Pins

A general trick that lock makers use to make picking harder is to modify the shape of the driver pin. The most popular shapes are mushroom, spool and serrated, see Figure 9.7. The purpose of these shapes is to cause the pins to false set low. These drivers stop a picking technique called vibration picking (see section 9.12), but they only slightly complicate scrubbing and one-pin-at-a-time picking (see chapter 4).

If you pick a lock and the plug stops turning after a few degrees and none of the pins

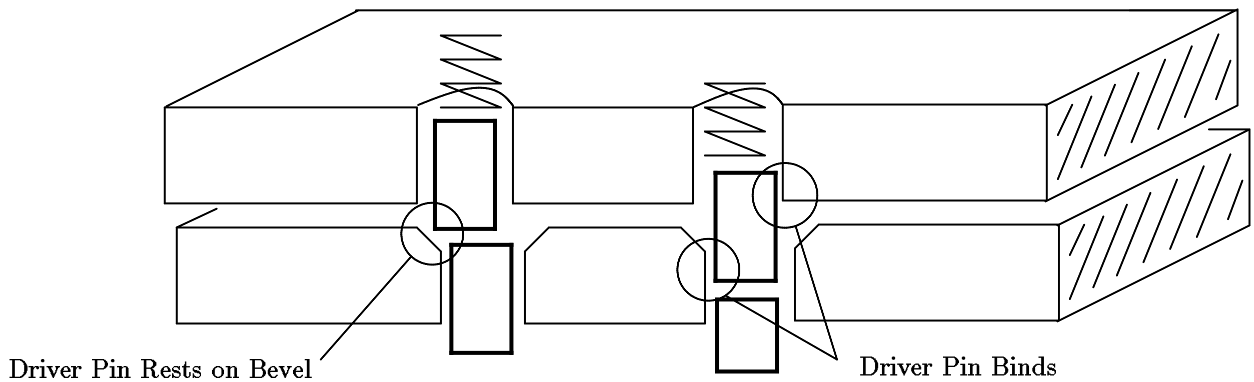


Figure 9.5: (a) Driver sets on bevel

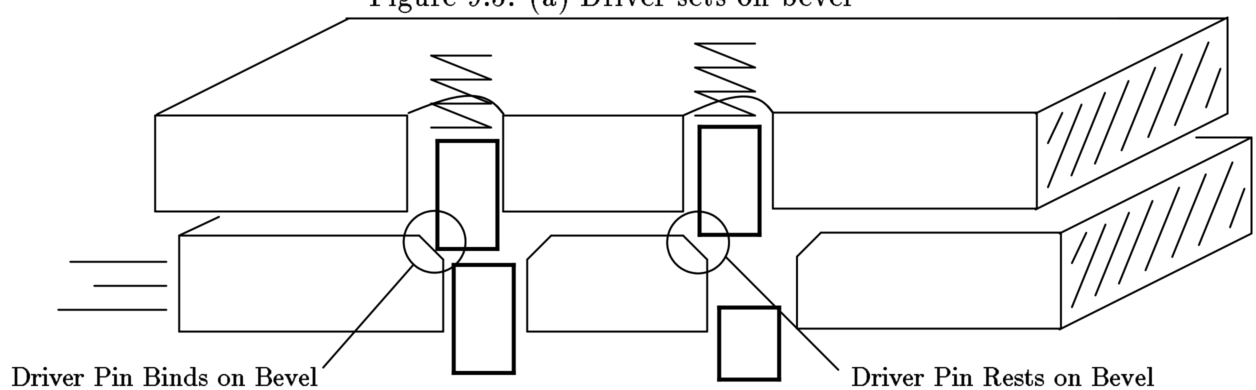


Figure 9.6: (b) Driver jams on bevel

can be pushed up any further, then you known that the lock has modified drivers. Basically, the lip of the driver has caught at the sheer line. See the bottom of Figure 9.7. Mushroom and spool drivers are often found in Russwin locks, and locks that have several spacers for master keying.

You can identify the positions with mushroom drivers by applying a light torque and pushing up on each pin. The pins with mushroom drivers will exhibit a tendency to bring the plug back to the fully locked position. By pushing the key pin up you are pushing the flat top of the key pin against the tilted bottom of the mushroom driver. This causes the driver to straighten up which in turn causes the plug to unrotate. You can use this motion to identify the columns that have mushroom drivers. Push those pins up to sheer line; even if you lose some of the other pins in the process they will be easier to re-pick than the pins with mushroom drivers. Eventually all the pins will be correctly set at the sheer line.

One way to identify all the positions with mushroom drivers is to use the flat of your pick to push all the pins up about halfway. This should put most of the drivers in their cockable position and you can feel for them.

To pick a lock with modified drivers, use a lighter torque and heavier pressure. You want to error on the side of pushing the key pins too far into the hull. In fact, another way to pick these locks is to use the flat side of your pick to push the pins up all the way, and apply very heavy torque to hold them there. Use a scrubbing action to vibrate the key pins while you slowly reduce the torque. Reducing the torque reduces the binding friction on the pins. The vibration and spring force cause the key pins to slide down to the sheer line.

The key to picking locks with modified drivers is recognizing incorrectly set pins. A mushroom driver set on its lip will not have the springy give of a correctly set driver. Practice recognizing the difference.

9.10 Master Keys

Many applications require keys that open only a single lock and keys that open a group of locks. The keys that open a single lock are called *change keys* and the keys that open multiple locks are called *master keys*. To allow both the change key and the master key to open the same lock, a locksmith adds an extra pin called a *spacer* to some of the pin columns. See Figure 9.8. The effect of the spacer is to create two gaps in the pin column that could be lined up with the sheer line. Usually the change key aligns the top of the spacer with the sheer line, and the master key aligns the bottom of the spacer with the sheer line (the idea is to prevent people from filing down a change key to get a master key). In either case the plug is free to rotate.

In general, spacers make a lock easier to pick. They increase the number of opportunities to set each pin, and they make it more likely that the lock can opened by setting the all the pins at about the same height. In most cases only two or three positions will have spacers. You can recognize a position with a spacer by the two clicks you feel when the pin is pushed down. If the spacer has a smaller diameter than the driver and key pins, then you will feel a wide springy region because the spacer will not bind as it passes through the sheer line. It is

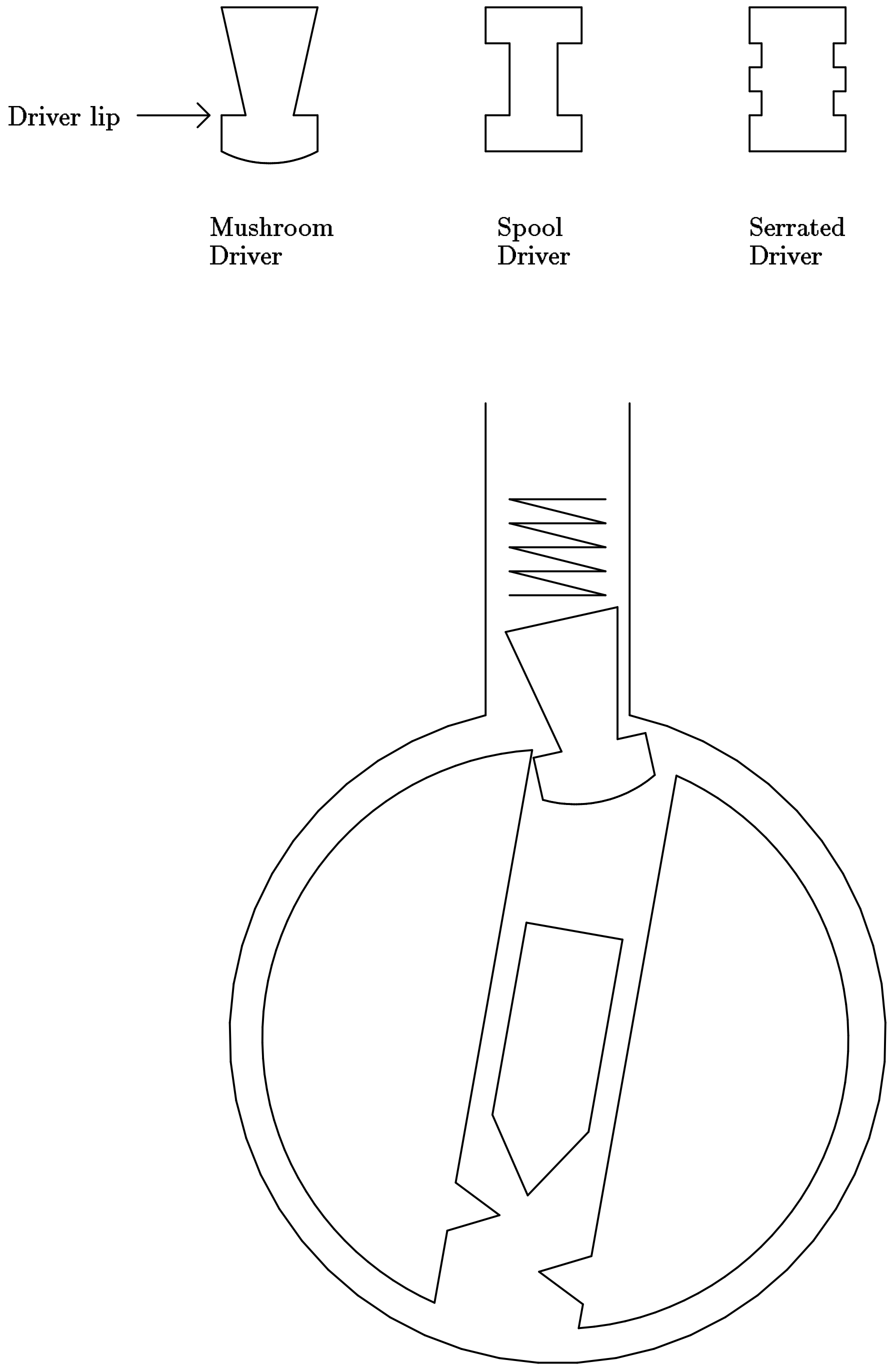


Figure 9.7: Mushroom, spool, and serrated driver pins

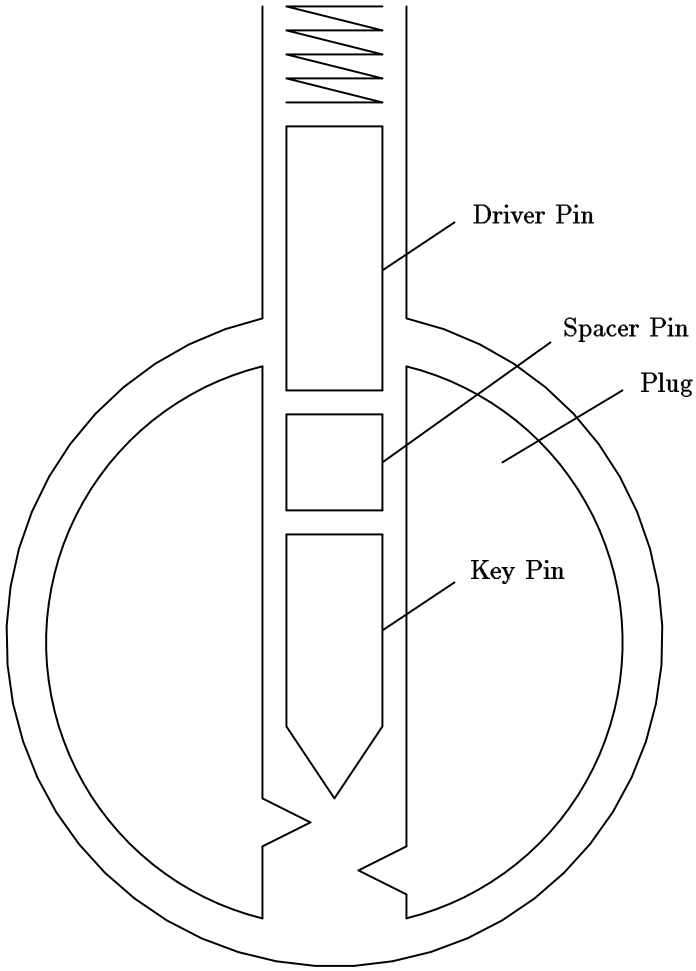


Figure 9.8: Spacer pins for master keying

more common for the spacer to be larger than the driver pin. You can recognize this by an increase in friction when the spacer passes through the sheer line. Since the spacer is larger than the driver pin, it will also catch better on the plug. If you push the spacer further into the hull, you will feel a strong click when the bottom of the spacer clears the sheer line.

Thin spacers can cause serious problems. If you apply heavy torque and the plug has beveled holes, the spacer can twist and jam at the sheer line. It is also possible for the spacer to fall into the keyway if the plug is rotated 180 degrees. See section 9.11 for the solution to this problem.

9.11 Driver or Spacer Enters Keyway

Figure 9.9 shows how a spacer or driver pin can enter the keyway when the plug is rotated 180 degrees. You can prevent this by placing the flat side of your pick in the bottom of the keyway **before** you turn the plug too far. If a spacer or driver does enter the keyway and prevent you from turning the plug, use the flat side of you pick to push the spacer back into

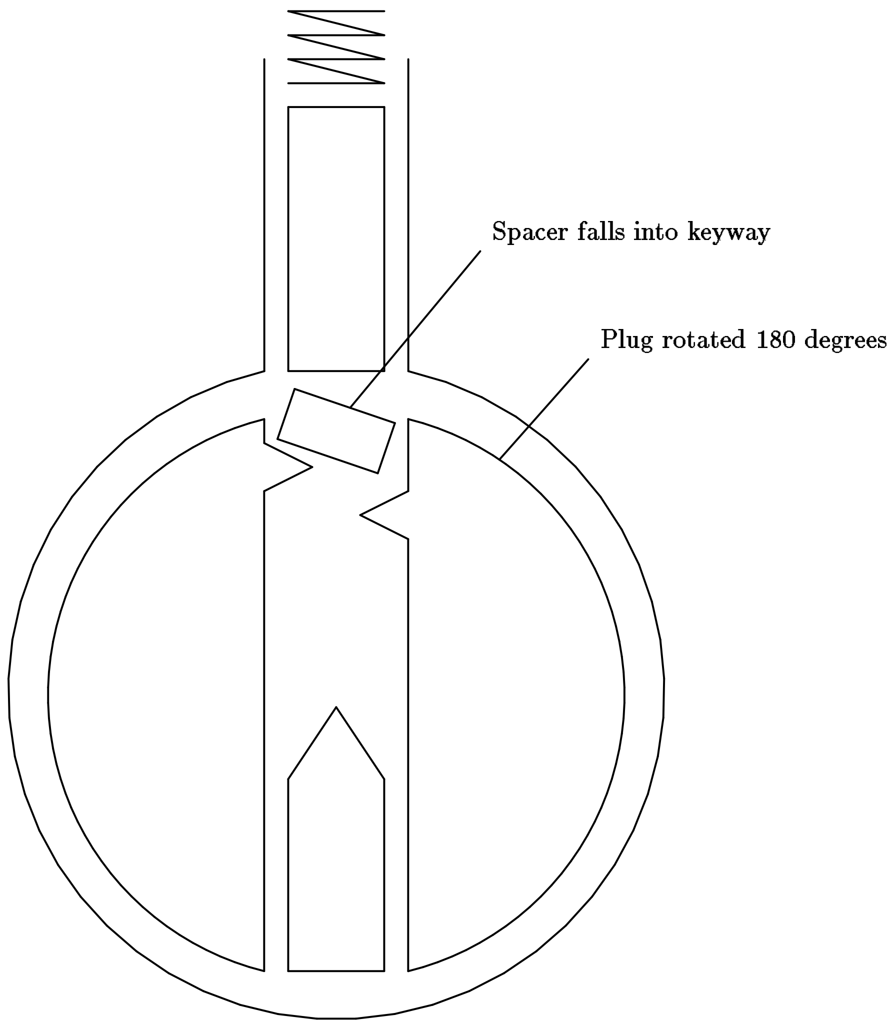


Figure 9.9: Spacer or driver can enter keyway

the hull. You may need to use the torque wrench to relieve any sheer force that is binding the spacer or driver. If that doesn't work try raking over the drivers with the pointed side of your pick. If a spacer falls into the keyway completely, the only option is to remove it. A hook shaped piece of spring steel works well for this, though a bent paperclip will work just as well unless the spacer becomes wedged.

9.12 Vibration Picking

Vibration picking works by creating a large gap between the key and driver pins. The underlying principle is familiar to anyone who has played pool. When the queue ball strikes another ball squarely, the queue ball stops and the other ball heads off with the same speed and direction as the queue ball. Now imagine a device that kicks the tips of all the key pins. The key pins would transfer their momentum to the driver pins which would fly up into the hull. If you are applying a light torque when this happens, the plug will rotate when all the

drivers are above the sheer line.

9.13 Disk Tumblers

The inexpensive locks found on desks use metal disks instead of pins. Figure 9.10 shows the basic workings of these locks. The disks have the same outline but differ in the placement of the rectangular cut.

These locks are easy to pick with the right tools. Because the disks are placed close together a half-round pick works better than a half-diamond pick (see Figure A.1). You may also need a torque wrench with a narrower head. Use moderate to heavy torque.

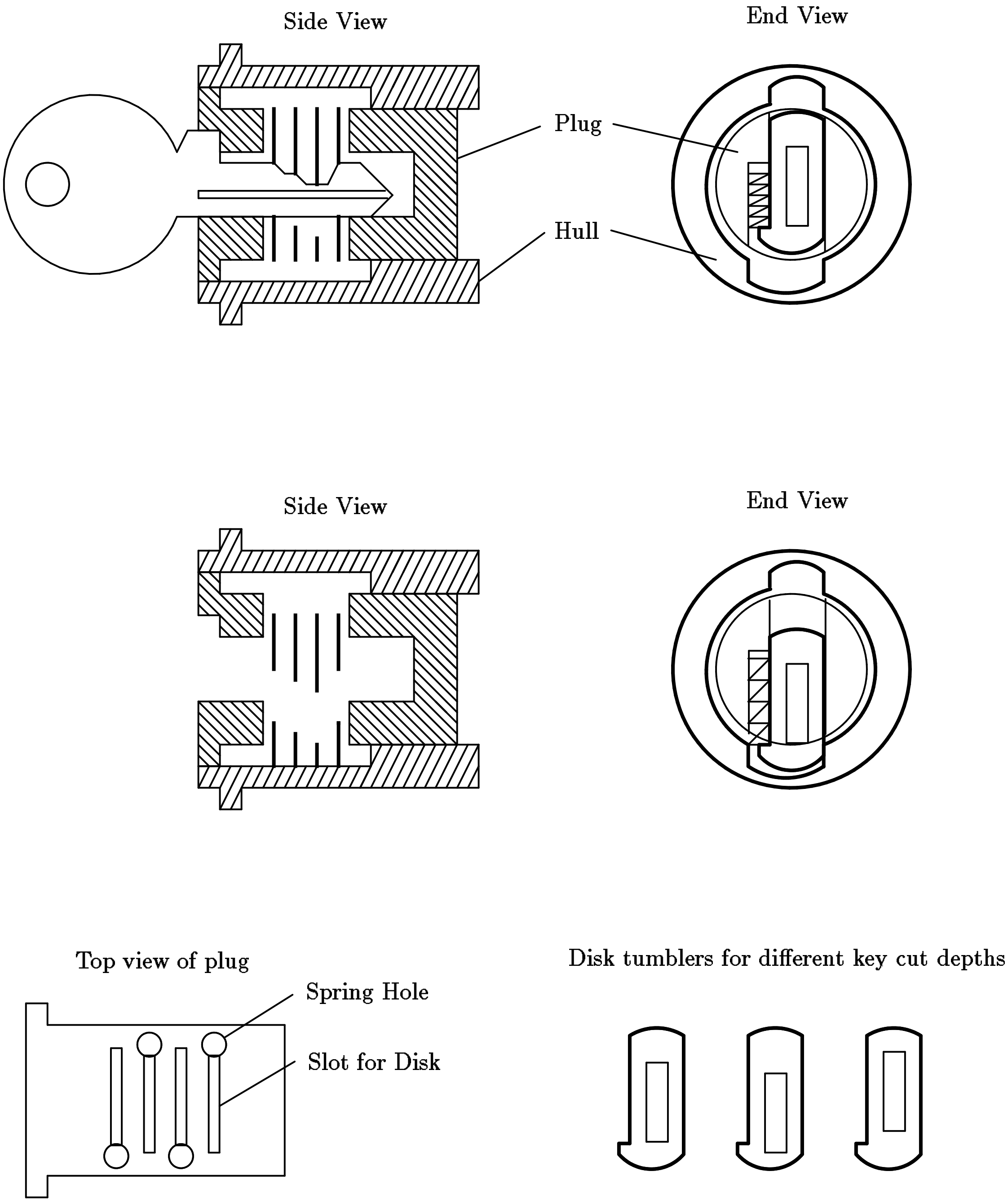


Figure 9.10: Workings of a disk tumbler lock

Chapter 10

Final Remarks

Lock picking is a craft, not a science. This document presents the knowledge and skills that are essential to lock picking, but more importantly it provides you with models and exercises that will help you study locks on your own. To excel at lock picking, you must practice and develop a style which fits you personally. Remember that the best technique is the one that works best for you.

Appendix A

Tools

This appendix describes the design and construction of lock picking tools.

A.1 Pick Shapes

Picks come in several shapes and sizes. Figure A.1 shows the most common shapes. The handle and tang of a pick are the same for all picks. The handle must be comfortable and the tang must be thin enough to avoid bumping pins unnecessarily. If the tang is too thin, then it will act like a spring and you will loose the feel of the tip interacting with the pins. The shape of the tip determines how easily the pick passes over the pins and what kind of feedback you get from each pin.

The design of a tip is a compromise between ease of insertion, ease of withdrawal and feel of the interaction. The half diamond tip with shallow angles is easy to insert and remove, so you can apply pressure when the pick is moving in either direction. It can quickly pick a lock that has little variation in the lengths of the key pins. If the lock requires a key that has a deep cut between two shallow cuts, the pick may not be able to push the middle pin down far enough. The half diamond pick with steep angles could deal with such a lock, and in general steep angles give you better feedback about the pins. Unfortunately, the steep angles make it harder to move the pick in the lock. A tip that has a shallow front angle and a steep back angle works well for Yale locks.

The half round tip works well in disk tumbler locks. See section 9.13. The full diamond and full round tips are useful for locks that have pins at the top and bottom of the keyway.

The rake tip is designed for picking pins one by one. It can also be used to rake over the pins, but the pressure can only be applied as the pick is withdrawn. The rake tip allows you to carefully feel each pin and apply varying amounts of pressure. Some rake tips are flat or dented on the top to makes it easier to align the pick on the pin. The primary benefit of picking pins one at a time is that you avoid scratching the pins. Scrubbing scratches the tips of the pins and the keyway, and it spreads metal dust throughout the lock. If you want to avoid leaving traces, you must avoid scrubbing.

The snake tip can be used for scrubbing or picking. When scrubbing, the multiple bumps

generate more action than a regular pick. The snake tip is particularly good at opening five pin household locks. When a snake tip is used for picking, it can set two or three pins at once. Basically, the snake pick acts like a segment of a key which can be adjusted by lifting and lowering the tip, by tilting it back and forth, and by using either to top or bottom of the tip. You should use moderate to heavy torque with a snake pick to allow several pins to bind at the same time. This style of picking is faster than using a rake and it leaves as little evidence.

A.2 Street cleaner bristles

The spring steel bristles used on street cleaners make excellent tools for lock picking. The bristles have the right thickness and width, and they are easy to grind into the desired shape. The resulting tools are springy and strong. Section A.3 describes how to make tools that are less springy.

The first step in making tools is to sand off any rust on the bristles. Course grit sand paper works fine as does a steel wool cleaning pad (not copper wool). If the edges or tip of the bristle are worn down, use a file to make them square.

A torque wrench has a head and a handle as shown in figure A.2. The head is usually 1/2 to 3/4 of an inch long and the handle varies from 2 to 4 inches long. The head and the handle are separated by a bend that is about 80 degrees. The head must be long enough to reach over any protrusions (such as a grip-proof collar) and firmly engage the plug. A long handle allows delicate control over the torque, but if it is too long, it will bump against the doorframe. The handle, head and bend angle can be made quite small if you want to make tools that are easy to conceal (e.g., in a pen, flashlight, or belt buckle). Some torque wrenches have a 90 degree twist in the handle. The twist makes it easy to control the torque by controlling how far the handle has been deflected from its rest position. The handle acts as a spring which sets the torque. The disadvantage of this method of setting the torque is that you get less feedback about the rotation of the plug. To pick difficult locks you will need to learn how to apply a steady torque via a stiff handled torque wrench.

The width of the head of a torque wrench determines how well it will fit the keyway. Locks with narrow keyways (e.g., desk locks) need torque wrenches with narrow heads. Before bending the bristle, file the head to the desired width. A general purpose wrench can be made by narrowing the tip (about 1/4 inch) of the head. The tip fits small keyways while the rest of the head is wide enough to grab a normal keyway.

The hard part of making a torque wrench is bending the bristle without cracking it. To make the 90 degree handle twist, clamp the head of the bristle (about one inch) in a vise and use pliers to grasp the bristle about 3/8 of an inch above the vise. You can use another pair of pliers instead of a vise. Apply a 45 degree twist. Try to keep the axis of the twist lined up with the axis of the bristle. Now move the pliers back another 3/8 inch and apply the remaining 45 degrees. You will need to twist the bristle more than 90 degrees in order to set a permanent 90 degree twist.

To make the 80 degree head bend, lift the bristle out of the vise by about 1/4 inch (so

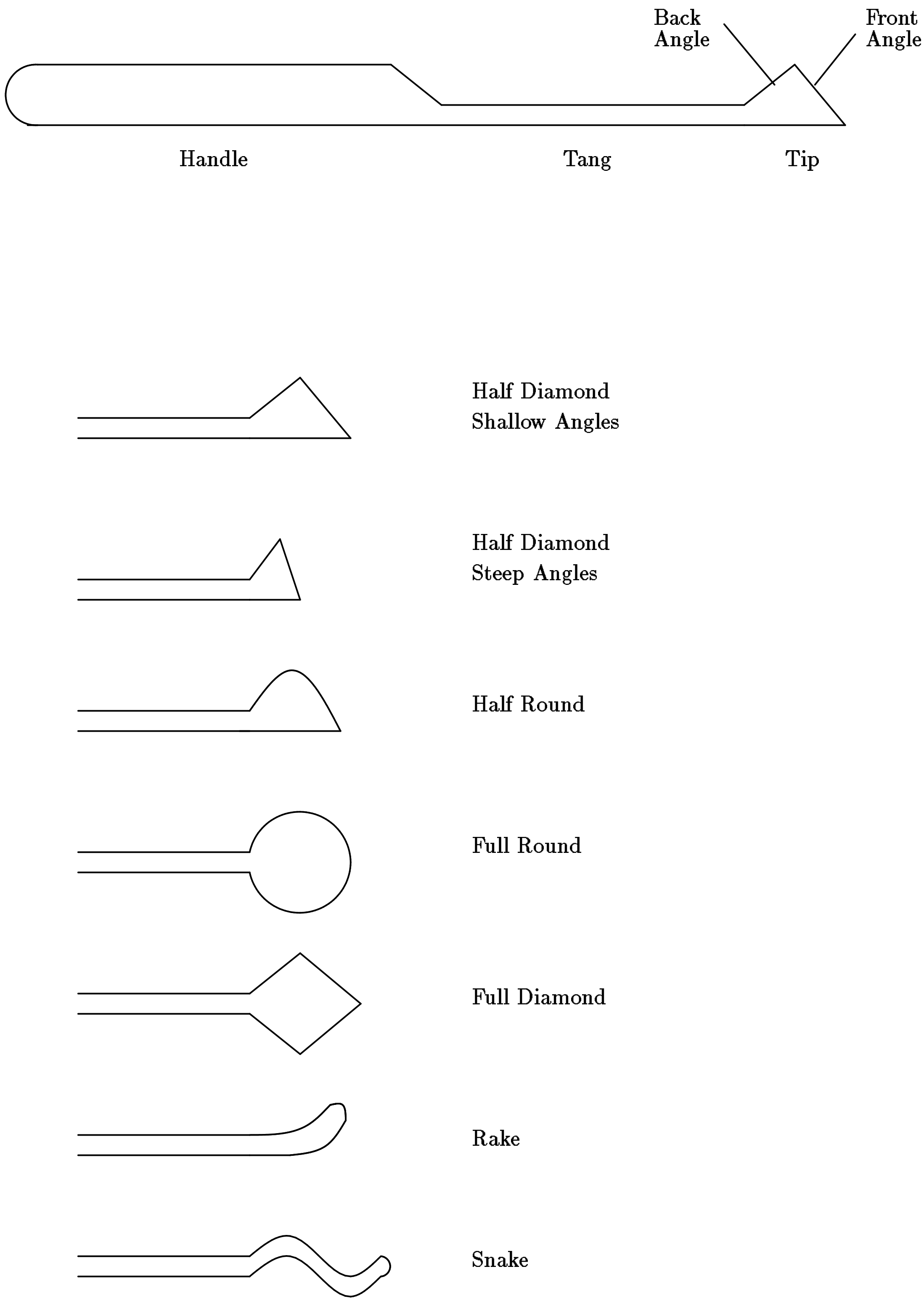


Figure A.1: Selection of pick shapes

3/4 inch is still in the vise). Place the shank of a screw driver against the bristle and bend the spring steel around it about 90 degrees. This should set a permanent 80 degree bend in the metal. Try to keep the axis of the bend perpendicular to the handle. The screwdriver shank ensures that the radius of curvature will not be too small. Any rounded object will work (e.g., drill bit, needle nose pliers, or a pen cap). If you have trouble with this method, try grasping the bristle with two pliers separated by about 1/2 inch and bend. This method produces a gentle curve that won't break the bristle.

A grinding wheel will greatly speed the job of making a pick. It takes a bit of practice to learn how make smooth cuts with a grinding wheel, but it takes less time to practice and make two or three picks than it does to hand file a single pick. The first step is to cut the front angle of the pick. Use the front of the wheel to do this. Hold the bristle at 45 degrees to the wheel and move the bristle side to side as you grind away the metal. Grind slowly to avoid overheating the metal, which makes it brittle. If the metal changes color (to dark blue), you have overheated it, and you should grind away the colored portion. Next, cut the back angle of the tip using the corner of the wheel. Usually one corner is sharper than the other, and you should use that one. Hold the pick at the desired angle and slowly push it into the corner of the wheel. The side of the stone should cut the back angle. Be sure that the tip of the pick is supported. If the grinding wheel stage is not close enough to the wheel to support the tip, use needle nose pliers to hold the tip. The cut should should pass though about 2/3 of the width of the bristle. If the tip came out well, continue. Otherwise break it off and try again. You can break the bristle by clamping it into a vise and bending it sharply.

The corner of the wheel is also used to grind the tang of the pick. Put a scratch mark to indicate how far back the tang should go. The tang should be long enough to allow the tip to pass over the back pin of a seven pin lock. Cut the tang by making several smooth passes over the corner. Each pass starts at the tip and moves to the scratch mark. Try to remove less than a 1/16th of an inch of metal with each pass. I use two fingers to hold the bristle on the stage at the proper angle while my other hand pushes the handle of the pick to move the tang along the corner. Use whatever technique works best for you.

Use a hand file to finish the pick. It should feel smooth if you run a finger nail over it. Any roughness will add noise to the feedback you want to get from the lock.

The outer sheath of phone cable can be used as a handle for the pick. Remove three or four of the wires from a length of cable and push it over the pick. If the sheath won't stay in place, you can put some epoxy on the handle before pushing the sheath over it.

A.3 Bicycle spokes

An alternative to making tools out of street cleaner bristles is to make them out of nails and bicycle spokes. These materials are easily accessible and when they are heat treated, they will be stronger than tools made from bristles.

A strong torque wrench can be constructed from an 8-penny nail (about .1 inch diameter). First heat up the point with a propane torch until it glows red, slowly remove it from the

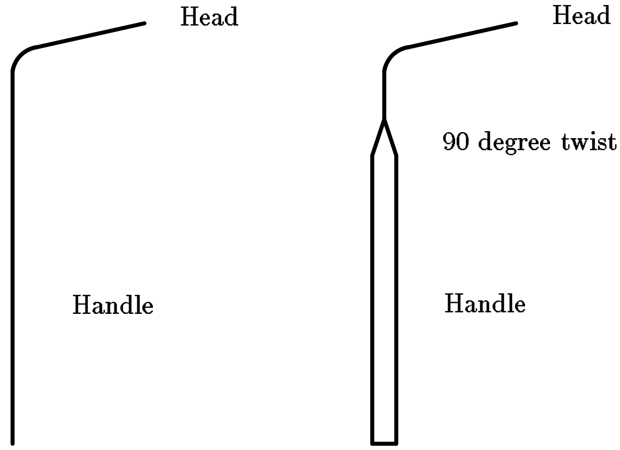


Figure A.2: Torque wrenches

flame, and let it air cool; this softens it. The burner of a gas stove can be used instead of a torch. Grind it down into the shape of a skinny screwdriver blade and bend it to about 80 degrees. The bend should be less than a right angle because some lock faces are recessed behind a plate (called an *escutcheon*) and you want the head of the wrench to be able to reach about half an inch into the plug. Temper (harden) the torque wrench by heating to bright orange and dunking it into ice water. You will wind up with a virtually indestructible bent screwdriver that will last for years under brutal use.

Bicycle spokes make excellent picks. Bend one to the shape you want and file the sides of the business end flat such that it's strong in the vertical and flexy in the horizontal direction. Try a right-angle hunk about an inch long for a handle. For smaller picks, which you need for those really tiny keyways, find any large-diameter spring and unbend it. If you're careful you don't have to play any metallurgical games.

A.4 Brick Strap

For perfectly serviceable key blanks that you can't otherwise find at the store, use the metal strap they wrap around bricks for shipping. It's wonderfully handy stuff for just about anything you want to manufacture. To get around side wards in the keyway, you can bend the strap lengthwise by clamping it in a vice and tapping on the protruding part to bend the piece to the required angle.

Brick strap is very hard. It can ruin a grinding wheel or key cutting machine. A hand file is the recommended tool for milling brick strap.

Appendix B

Legal Issues

Contrary to widespread myth, it is not a felony to possess lockpicks. Each state has its own laws with respect to such burglarious instruments. Here is the Massachusetts version quoted in entirety from the massachusetts general code:

Chapter 266 (crimes against property)
Section 49. Burglarious instruments; making; possession; use.

> Whoever makes or mends, or begins to make or mend, or knowingly has in his possession, an engine, machine, tool or implement adapted and designed for cutting through, forcing or breaking open a building, room, vault, safe or other depository, IN ORDER TO STEAL THEREFROM money or other property, or to commit any other crime, knowing the same to be adapted and designed for the purpose aforesaid, WITH INTENT TO USE OR EMPLOY OR ALLOW the same to be used or employed for such purpose, or whoever knowingly has in his possession a master key designed to fit more than one motor vehicle, WITH INTENT, TO USE OR EMPLOY THE SAME to steal a motor vehicle or other property therefrom, shall be punished by imprisonment in the state prison for not more than ten years or by a fine of not more than one thousand dollars and imprisonment in jail for not more than two and one half years.

Emphasis added.

In other words, mere possession means nothing. If they stop you for speeding or something, and find a pick set, they can't do much. On the other hand, if they catch you picking the lock on a Monec machine they get to draw and quarter you.

States with similar wording include ME, NH, NY. One place that DOES NOT have similar wording, and does make possession illegal, is Washington, DC. These are the only other places I have checked. I would imagine that most states are similar to Massachusetts, but I would not bet anything substantial (say, more than a slice of pizza) on it.

It may be a good idea to carry around a xeroxed copy of the appropriate page from your state's criminal code.